Docket No.: 58799-096 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	Customer Number: 20277
Tatsuya FUJIYAMA, et al.	:	Confirmation Number:
Serial No.:	:	Group Art Unit:
Filed: September 30, 2003	:	Examiner:

For: SECURITY SPECIFICATION CREATION SUPPORT DEVICE AND METHOD OF SECURITY SPECIFICATION CREATION SUPPORT

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Mail Stop
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2003-134706, filed May 13, 2003

cited in the Declaration of the present application. A Certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Keith E. George
Registration No. 34,111

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 KEG:prg
Facsimile: (202) 756-8087
Date: September 30, 2003

58799-096
Fujiyama et al.
Sept. 30, 2003

McDermott, Will & Emery

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　５月１３日

出願番号
Application Number: 特願２００３－１３４７０６

[ST. 10/C]: [ＪＰ２００３－１３４７０６]

出願人
Applicant(s): 株式会社日立製作所

２００３年　７月　９日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５５２２８

【書類名】　特許願
【整理番号】　HK14929000
【提出日】　平成15年 5月13日
【あて先】　特許庁長官　　殿
【国際特許分類】　G06F　9/06
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　藤山　達也
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　永井　康彦
【発明者】
　【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内
　【氏名】　根本　繁幸
【特許出願人】
　【識別番号】　000005108
　【氏名又は名称】　株式会社　日立製作所
【代理人】
　【識別番号】　100084032
　【弁理士】
　【氏名又は名称】　三品　岩男
　【電話番号】　045(316)3711
【手数料の表示】
　【予納台帳番号】　011992
　【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】明細書

【発明の名称】セキュリティ仕様書作成支援装置、および、セキュリティ仕様書作成支援方法

【特許請求の範囲】

【請求項１】

情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するセキュリティ仕様書作成支援装置であって、

既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースと、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付手段と、

前記コンポーネント各々について、前記定義情報受付手段で受付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、

所定のセキュリティ仕様書の雛形に、前記セキュリテ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受付けるセキュリティ仕様書原案作成手段と、を有すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項２】

請求項１記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書選定手段は、

前記コンポーネント各々について、前記セキュリティ仕様書事例データベースから再利用可能な事例を少なくとも１つ検出できた場合、検出できた事例のなかから再利用する事例をユーザに選定させ、当該選定された事例を当該コンポーネントのセキュリティ仕様書原案とすると共に、当該原案の修正をユーザより受付け、前記セキュリティ仕様書事例データベースから再利用可能な事例を検出できなかった場合、当該コンポーネントのセキュリティ仕様書原案をユーザより受付けることで、前記コンポーネント各々のセキュリティ仕様書原案を作成し、

前記セキュリティ仕様書原案作成手段は、

前記セキュリティ仕様書の雛形に、前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、前記コンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項３】

請求項２記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書原案作成手段は、

前記コンポーネント各々のセキュリティ仕様書原案の記述の記載箇所を特定できるように、前記コンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項４】

請求項１記載のセキュリティ仕様書作成支援装置であって、

前記定義情報受付手段は、

前記情報ネットワークシステムを運用環境単位で分割することで得られるドメイン各々の定義情報と、前記ドメイン各々について、当該ドメインを装置単位で分割することで得られるサブシステム各々の定義情報と、前記サブシステム各々について、当該サブシステムをセキュリティ分析上の最小単位で分割することで得られるコンポーネント各々の定義情報とを、ユーザより受付けること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項５】

請求項４記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書原案作成手段は、

所定のセキュリティ仕様書の雛形に、前記ドメインあるいは前記サブシステムに属する前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、当該ドメインあるいは当該サブシステムのコンポジットセキュリティ仕様書原案を作成すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項６】

請求項５記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書事例データベースには、

過去に作成されたドメインおよびサブシステムのコンポジットセキュリティ仕様書が事例として登録されており、

前記セキュリティ仕様書選定手段は、

前記ドメイン各々あるいは前記サブシステム各々について、前記定義情報受付手段で受付けた当該ドメインあるいは当該サブシステムの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能なドメインあるいはサブシステムのコンポジットセキュリティ仕様書の事例を検索すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項７】

請求項４記載のセキュリティ仕様書作成支援装置であって、

複数のサブシステム各々についてコンポーネント構成の典型パターンが事例として登録されたシステム構成事例データベースをさらに有し、

前記定義情報受付手段は、

ユーザより受付けたサブシステムの定義情報に基づいて、前記システム構成事例から当該サブシステムのコンポーネント構成の典型パターンを特定し、特定した典型パターンのコンポーネント構成が示すコンポーネント各々について、ユーザより定義情報を受付けること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項８】

請求項４記載のセキュリティ仕様書作成支援装置であって、

前記定義情報受付手段により定義情報を受付けたドメイン、サブシステムおよびコンポーネントの各々を、前記情報ネットワークシステムにおける階層関係が識別可能なツリー構造で表示するツリー表示手段を有すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項９】

請求項８記載のセキュリティ仕様書作成支援装置であって、

前記ツリー表示手段は、

同一のサブシステムを構成するコンポーネントの各々を、前記サブシステムにおける階層関係が識別可能なレイヤ構造で表示すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項１０】

請求項８記載のセキュリティ仕様書作成支援装置であって、

前記ツリー表示手段は、

コンポーネント各々を、前記セキュリティ仕様書選定手段による事例の検出の有無が識別可能に表示すること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項１１】

請求項１記載のセキュリティ仕様書作成支援装置であって、

前記セキュリティ仕様書事例データベースは、ネットワークを介して、前記セキュリティ仕様書選定手段から離れて配置されていること

を特徴とするセキュリティ仕様書作成支援装置。

【請求項１２】

情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するためのコンピュータで読取り可能なプログラムであって、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付手段と、

前記コンポーネント各々について、前記定義情報受付手段で受付けた当該コンポーネントの定義情報に基づいて、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、

所定のセキュリティ仕様書の雛形に、前記セキュリテ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受付けるセキュリティ仕様書原案作成手段として、前記コンピュータを機能させること

を特徴とするコンピュータで読取り可能なプログラム。

【請求項１３】

コンピュータを用いて情報ネットワークシステムに対するセキュリティ仕様書の作成を支援するセキュリティ仕様書作成支援方法であって、

前記コンピュータあるいはネットワークを介して前記コンピュータに接続された他のコンピュータの記憶装置には、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースが格納されており、

前記コンピュータの演算装置は、

前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付ステップと、

前記コンポーネント各々について、前記定義情報受付ステップで受付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定ステップと、

所定のセキュリティ仕様書の雛形に、前記セキュリテ仕様書選定ステップで検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受付けるセキュリティ仕様書原案作成ステップと、を行うこと

を特徴とするセキュリティ仕様書作成支援方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、セキュリティ仕様書、特に、国際セキュリティ評価基準ＩＳＯ１５４０８に従ったセキュリティ仕様書の作成を支援する技術に関する。

【０００２】

【従来の技術】

ＩＴ（Information Technology）製品のセキュリティ機能の設計・評価に関する基準として、国際セキュリティ評価基準ＩＳＯ/ＩＥＣ１５４０８（ＣＣ：Common Criteria）がある。このＩＳＯ１５４０８に準拠した製品の開発を行い、その評価・認証を取得するためには、ＩＳＯ１５４０８特有のセキュリティ要求仕様書（ＰＰ:Protection Profile）またはセキュリティ設計仕様書（ＳＴ:Security Target）を作成することが必須となっている。以下では、セキュリティ要求

仕様書およびセキュリティ設計仕様書を、セキュリティ仕様書と呼ぶこととする。これらのセキュリティ仕様書を作成するには、セキュリティ全般およびＩＳＯ１５４０８に関する専門知識は勿論のこと、対象製品に固有の脅威や対策事例に関する豊富な知識や、どの脅威に対してどの対策が有効であるかといったセキュリティに関するノウハウや、リスク分析等の分析業に関わる専門技術が必要であるという問題がある。また、リスク分析等の分析作業の実施には、脅威や対策等に対して抜け漏れのない洗い出しや、対策のための適切なセキュリティ要件の選択などが必要であり、このため、膨大な時間を要するという問題もある。

【０００３】

これらの問題に対応するＩＳＯ１５４０８準拠のセキュリティ設計支援ツールとして、米国のセキュリティ認証機関であるＮＩＡＰ（The National Information Assurance Partnership）によるＣＣ ＴｏｏｌＢｏｘ(TM)（商標権者：National Security Agency)や、非特許文献１や、特許文献１に記載のものがある。

【０００４】

ＣＣ ＴｏｏｌＢｏｘ(TM)や非特許文献１に記載のセキュリティ設計支援ツールは、セキュリティ仕様書に記載する脅威やセキュリティ対策方針等の各種定義情報の事例を事前登録したデータベースを用意し、そのデータベースからユーザが直接選択した定義情報や、提示された質問にユーザが答えることによってデータベースから抽出された定義情報を、セキュリティ仕様書の所定箇所に自動的に記載する。これにより、定義情報をユーザが自ら考案する負担を低減しつつ、所定形式に沿ったセキュリティ仕様書を自動作成することができる。

【０００５】

また、特許文献１に記載のセキュリティ設計支援ツールは、評価・認証後に登録機関によって管理される認証済みのセキュリティ仕様書や、過去に作成した既存のセキュリティ仕様書をデータベース化し、脅威等の各種定義情報の事例を個別に再利用できるようにするだけではなく、認証済みのセキュリティ仕様書の定義情報一式も再利用できるようにしている。このようにすることで、仕様書作成時のリスク分析等の作業負担を低減することができる。

【０００６】

【非特許文献１】

「セキュリティ設計評価支援ツール(V3.0) 利用者マニュアル」、情報処理振興事業協会セキュリティセンター、２００２年５月、ｐ.2-６９

【特許文献１】

特開２００１-２２２４２０号公報

【０００７】

【発明が解決しようとする課題】

上述した従来のセキュリティ設計支援ツールは、個々のＩＴ製品に対するセキュリティ仕様書の作成を支援することを前提にしている。複数のＩＴ製品を構成要素とする情報ネットワークシステムでは、既存のＩＴ製品と新規開発のＩＴ製品とが混在している場合もある。上述した従来のセキュリティ設計支援ツールは、このような情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することについて考慮されていない。

【０００８】

本発明は上記事情に鑑みてなされたものであり、本発明の目的は、複数のＩＴ製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することにある。

【０００９】

【課題を解決するための手段】

上記課題を解決するために、本発明は、情報ネットワークシステムを構成する各コンポーネントの定義情報をユーザより受付ける。次に、コンポーネント各々について、既存のセキュリティ仕様書を蓄積したデータベースに再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。それから、予め用意してあるセキュリティ仕様書の雛形に前記特定したセキュリティ仕様書各々の内容を反映して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書の原案を自動生成し、ユーザに提示する。そして、ユーザよりコンポジットセキュリティ仕様書の原案の修正を受付ける。このようにすることで、専門知識・技術やノウハウを持もたないユーザが情報ネットワークシステムのセキュリティ仕様書原案を作成することを支援する。

【００１０】

例えば、本発明のセキュリティ仕様書作成支援装置は、既存のセキュリティ仕様書が事例として登録されたセキュリティ仕様書事例データベースと、前記情報ネットワークシステムを構成するコンポーネント各々の定義情報をユーザより受付ける定義情報受付手段と、前記コンポーネント各々について、前記定義情報受付手段で受付けた当該コンポーネントの定義情報に基づいて、前記セキュリティ仕様書事例データベースから再利用可能な事例を検索するセキュリティ仕様書選定手段と、所定のセキュリティ仕様書の雛形に、前記セキュリテ仕様書選定手段が検索した事例各々の内容を記述して、情報ネットワークシステムに対するコンポジットセキュリティ仕様書原案を作成すると共に、当該原案の修正をユーザより受付けるセキュリティ仕様書原案作成手段と、を有する。

【００１１】

ここで、前記セキュリティ仕様書選定手段は、前記コンポーネント各々について、前記セキュリティ仕様書事例データベースから再利用可能な事例を少なくとも１つ検出できた場合、検出できた事例のなかから再利用する事例をユーザに選定させ、当該選定された事例を当該コンポーネントのセキュリティ仕様書原案とすると共に、当該原案の修正をユーザより受付け、前記セキュリティ仕様書事例データベースから再利用可能な事例を検出できなかった場合、当該コンポーネントのセキュリティ仕様書原案をユーザより受付けることで、前記コンポーネント各々のセキュリティ仕様書原案を作成してもよい。また、前記セキュリティ仕様書原案作成手段は、前記セキュリティ仕様書の雛形に、前記コンポーネント各々のセキュリティ仕様書原案の内容を記述して、前記コンポジットセキュリティ仕様書原案を作成してもよい。

【００１２】

また、前記定義情報受付手段は、前記情報ネットワークシステムを運用環境単位で分割することで得られるドメイン各々の定義情報と、前記ドメイン各々について、当該ドメインを装置単位で分割することで得られるサブシステム各々の定義情報と、前記サブシステム各々について、当該サブシステムをセキュリティ分析上の最小単位で分割することで得られるコンポーネント各々の定義情報とを、

ユーザより受付けるようにしてもよい。

【００１３】

また、前記セキュリティ仕様書事例データベースは、ネットワークを介して、前記セキュリティ仕様書選定手段から離れて配置されているようにしてもよい。

【００１４】

【発明の実施の形態】

以下、本発明の実施形態について説明する。

【００１５】

図１は、本発明の一実施形態が適用されたセキュリティ仕様書作成支援装置１１により、コンポジットセキュリティ仕様書原案の作成対象である情報ネットワークシステム（設計対象システムと呼ぶ）１６に対するコンポジットセキュリティ仕様書原案が作成されるまでの大まかな処理の流れ（原理）を示している。

【００１６】

本実施形態のセキュリティ仕様書作成支援装置１１は、設計対象システム１６のシステム構成等のシステム計画・設計段階における情報に基づいて、再利用可能な既存のセキュリティ仕様書を選定し、これらを利用して設計対象システムに対するコンポジットセキュリティ仕様書の作成を支援する。

【００１７】

図示するように、セキュリティ仕様書作成支援装置１１は、設計対象システム１６を定義するシステム構成定義機能１１１と、セキュリティ仕様書の事例が登録された仕様書事例ＤＢ（データベース）１２からコンポジットセキュリティ仕様書原案に再利用可能なセキュリティ仕様書を選定するセキュリティ仕様書選定機能１１２と、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動作成するセキュリティ仕様書原案作成機能１１３と、を有する。

【００１８】

システム構成定義機能１１１は、例えばＧＵＩ（Graphical User Interface）を介してユーザより設計対象システム１６の階層構造を示す定義情報を受付ける。具体的には、ユーザの指示に従い、設計対象システム１６を、ドメイン（例えば地理的条件や会社の組織構成といった運用環境単位で分類される構成要素）の

階層１６１、サブシステム（例えばＩＴ製品、ネットワークといった装置単位で分類される構成要素）の階層１６２、および、コンポーネント（ソフト部品、ハード部品といったセキュリティ分析上の最小単位で分類される構成要素）の階層１６３の３つ階層に分ける。そして、階層１６１～１６３毎に、構成要素の定義情報をユーザより受付ける。ドメインの階層１６１ならば、各ドメイン１～Ｌの運用方針および他ドメインとのインターフェースに関するドメイン間対応情報を各ドメイン１～Ｌの定義情報として受付ける。サブシステムの階層１６２ならば、各サブシステム１～Ｍの所属ドメインおよびサブシステム間対応情報を各サブシステム１～Ｍの定義情報として受付ける。そして、コンポーネントの階層１６３ならば、各コンポーネント１～Ｎの所属サブシステム、コンポーネント固有情報およびコンポーネント間対応情報を各コンポーネント１～Ｎの定義情報として受付ける。

【００１９】

仕様書事例ＤＢ１２には、既存のセキュリティ仕様書（認証済みセキュリティ仕様書、過去に作成したセキュリティ仕様書、業界標準や顧客の要件を記述したセキュリティ仕様書等）が事例として登録されている。セキュリティ仕様書選定機能１１２は、コンポーネント各々について、定義情報と適合する事例を仕様書事例ＤＢ１２から検索する。そして、コンポーネント各々について、ユーザよりの指示に従い、検索した事例の中からコンポジットセキュリティ仕様書原案に再利用可能な既存のセキュリティ仕様書１７を選定する。

【００２０】

セキュリティ仕様書原案作成機能１１３は、コンポーネント各々について、当該コンポーネントに対して選定された既存のセキュリティ仕様書１７を、当該コンポーネントに対するセキュリティ仕様書原案１９とする。このとき、既存のセキュリティ仕様書１７が選定されなかったコンポーネントについては、ユーザが新規作成したセキュリティ仕様書を、当該コンポーネントに対するセキュリティ仕様書原案１９とする。また、予め用意してあるセキュリティ仕様書の雛形に、各コンポーネントのセキュリティ仕様書原案１９各々の内容を反映する。これより、コンポジットセキュリティ仕様書原案１８および各コンポーネントのセキュ

リティ仕様書原案１９を有するシステムセキュリティ仕様書原案１３を自動生成する。そして、システムセキュリティ仕様書原案１３を、例えばＧＵＩを介してユーザに提示して編集を受付ける。

【００２１】

図２は、設計対象システムの一例を示す図である。

【００２２】

図２に示す設計対象システムの例は、社員の勤休管理を行う情報ネットワークシステム（勤休管理システム）である。この勤休管理システムを構成するＩＴ製品は、本社拠点区域２１に存在するものと、支社拠点区域２２に存在するものとに分類することができる。

【００２３】

本社拠点区域２１に属するＩＴ製品としては、本社ビル２１５内に存在する一般利用者端末２１１、本社ビル２１５の情報機器室２１６内に存在する勤休管理サーバ機器２１２および社員情報ＤＢ２１３、および、本社拠点区域２１内の各ＩＴ製品を接続する拠点内ネットワーク２１４がある。一方、支社拠点区域２２に属するＩＴ製品としては、支社ビル２２３内に存在する一般利用者端末２２１、および、支社拠点区域２２内の各ＩＴ製品を接続する拠点内ネットワーク２２２がある。そして、拠点内ネットワーク２１４および拠点内ネットワーク２２２は拠点間ネットワークであるインターネット２３を介して相互接続されている。

【００２４】

また、一般利用者端末２１１、２２１を構成する部品としては、ＡＴ互換ハードウェア２１１４、ネットワークカード２１１５、ＡＴ互換ハードウェア２１１４上で動作する端末ＯＳ２１１３、端末ＯＳ２１１３上で動作する勤休入力用ブラウザ２１１１、および、端末ＯＳ２１１３上で動作する通知受信用メーラ２１１２がある。一方、勤休管理サーバ機器２１２を構成する部品としては、ＡＴ互換ハードウェア２１２５、ネットワークカード２１２６、ＡＴ互換ハードウェア２１２５上で動作するサーバＯＳ２１２４、サーバＯＳ２１２４上で動作するＤＢＭＳ（DataBase Management System）２１２３、ＤＢＭＳ２１２３上で動作する勤休管理用サーバ２１２１、および、ＤＢＭＳ２１２３上で動作するメールサ

ーバ２１２２がある。

【００２５】

以上のような構成を有する勤休管理システムにおいて、一般社員は一般利用者端末２１１、２２１の勤休入力用ブラウザ２１１１を使用して勤休管理サーバ２１２にアクセスし、勤休情報を登録・参照することができる。また、一般利用者端末２１１、２２１の通知受信用メーラ２１１２により、登録情報の修正依頼等の通知を受信することができる。

【００２６】

図３は、セキュリティ仕様書作成支援装置１１が作成を支援するセキュリティ仕様書を説明するための図である。

【００２７】

ここで、図３（Ａ）は、国際セキュリティ評価基準ＩＳＯ１５４０８に従ったセキュリティ仕様書（ＰＰ/ＳＴ）の構成例３１および各種定義情報の記述例３３を示している。図示するように、ＩＳＯ１５４０８準拠のセキュリティ仕様書には、仕様書タイトル３１１、対象製品名３１２、ＴＯＥ（Target of Evaluation）３１３、前提条件３３１、組織のセキュリティ方針３３２、および、評価保証レベル３３３を含む複数の所定の項目が設けられている。ＩＳＯ１５４０８準拠のセキュリティ仕様書では、目次構成および各目次におかる記述内容が規定されている。このため、目的の情報がどの目次にあるかを特定できれば、セキュリティ仕様書から目的の情報を適切に参照したり抽出したりすることができる。

【００２８】

図３（Ｂ）は、コンポジットセキュリティ仕様書の一例３５を示している。図示するように、コンポジットセキュリティ仕様書は、国際セキュリティ評価基準ＩＳＯ１５４０８に準拠している。上述したように、本実施形態のセキュリティ仕様書作成支援装置１１が作成を支援するシステムセキュリティ仕様書原案１３は、設計対象システム１６を構成する各コンポーネントのセキュリティ仕様書原案１９および設計対象システムのコンポジットセキュリティ仕様書原案１８を備えて構成される。そして、コンポジットセキュリティ仕様書原案１８は、設計対象システムのセキュリティ環境記述に該当する記述のあるコンポーネントのセキ

ュリティ仕様書原案１９や、設計対象システムのセキュリティ対策方針、セキュリティ要件およびセキュリティ機能を実現するコンポーネントのセキュリティ仕様書原案１９の記述内容が参照（反映）されるように自動生成される。このようにして、システム全体について抜け漏れなく記述するものである。コンポジットセキュリティ仕様書の一例３５では、各コンポーネントのセキュリティ仕様書の記述内容が参照されている部分（下線３５１が引いてある部分）を特定可能なように、コンポジットセキュリティ仕様書が作成されている。

【００２９】

図４は、本実施形態のセキュリティ仕様書作成支援装置１１の概略構成図である。図示するように、本実施形態のセキュリティ仕様書作成支援装置１１は、ＣＰＵ５１と、メモリ５２と、ＨＤＤ等の外部記憶装置５４と、ＬＣＤ、ＣＲＴ等の表示装置５６およびキーボード、マウス等の入力装置５７を介してユーザに情報を提示したり、ユーザから情報を受付けたりする端末入出力装置５２と、ネットワークを介して通信を行うためのネットワークＩＦ（インターフェース）装置５８と、ＣＤ-ＲＯＭ、ＤＶＤ-ＲＯＭ、ＭＯ、フレキシブルディスク等の可搬記憶媒体の読込み・書出しを制御する可搬記憶媒体入出力装置５９と、これらの各装置を相互接続するバス５３と、を備えた通常のコンピュータシステムにおいて、ＣＰＵ５１がメモリ５５にロードされた通信制御ＰＧ（プログラム）５４１およびセキュリティ仕様書作成支援ＰＧ５４２を実行することで実現される。

【００３０】

ここで、通信制御ＰＧ５４１は、ＣＰＵ５１がネットワークＩＦ装置５８を介してネットワークに接続された他のネットワーク端末と通信を行うためのプログラムである。また、セキュリティ仕様書作成支援ＰＧ５４２は、図１に示すシステム構成定義機能１１１、セキュリティ仕様書選定機能１１２およびセキュリティ仕様書原案作成機能１１３を実現するためのプログラムである。本実施形態では、セキュリティ仕様書作成支援ＰＧ５４２を、システム構成定義機能１１１を実現するためのシステム構成定義ＰＧ５４２１、セキュリティ仕様書選定機能１１２を実現するためのセキュリティ仕様書選定ＰＧ５４２２、および、セキュリティ仕様書原案作成機能１１３を実現するためのセキュリティ仕様書原案作成Ｐ

Ｇ５４２３の、３つのプログラムを含めて構成している。通信制御ＰＧ５４１およびセキュリティ仕様書作成支援ＰＧ５４２は、例えば外部記憶装置５４あるいは可搬記憶媒体５９１に予め格納される。そして、外部記憶装置５４から、あるいは、可搬記憶媒体入出力装置５９を介して可搬記憶媒体５９から、メモリ５５上にロードされる。

【００３１】

外部記憶装置５４あるいは可搬記憶媒体５９１には、各種ＤＢ５４３～５４５が格納される。セキュリティ仕様書事例ＤＢ５４３には、認証済みセキュリティ仕様書、過去に作成したセキュリティ仕様書、および、業界標準や顧客の要件を記述したセキュリティ仕様書を含む既存のセキュリティ仕様書が事例として登録されており、図１に示す仕様書事例ＤＢ１２に相当する。

【００３２】

図５は、セキュリティ仕様書事例ＤＢ５４３のデータ管理の仕組みを説明するための図である。図示するように、セキュリティ仕様書事例ＤＢ５４３は、既存のセキュリティ仕様書の事例が、コンポーネントの種類を示すカテゴリ５４３１および同一種類のコンポーネントの形式を示すタイプ５４３２をキーとして検索できるようにデータベース化されている。

【００３３】

システム構成事例ＤＢ５４４には、情報ネットワークシステムを構成する各サブシステムの典型的なシステム展開パターンがシステム構成事例として登録されている。ここで、システム展開パターンとはサブシステムのツリー構成を特定するためのデータであり、システム展開パターンによりサブシステムを構成する各コンポーネントを特定できる。

【００３４】

図６は、システム構成事例ＤＢ５４４の登録例を示す図である。図示するように、本実施形態では、システム展開パターン５４４１をタグ形式で記述している。ここで、＜サブシステム＞タグ５４４３ａおよび＜/サブシステム＞５４４３ｂで囲まれた領域に、サブシステムの名称および該システムを構成する各コンポーネントの情報が記述され、＜サブシステム＞タグ５４４３ａの次に位置する２

つのタグ＜要素名＞、＜/要素名＞で囲まれた領域５４４６に、サブシステムのタイプが記述される。また、＜コンポーネント＞タグ５４４４ａおよび＜/コンポーネント＞５４４４ｂで囲まれた領域に、コンポーネントの名称および該コンポーネントの定義や仕様書に関する情報が記述され、＜コンポーネント＞タグ５４４４ａの次に位置する２つのタグ＜要素名＞、＜/要素名＞で囲まれた領域５４４７に、コンポーネントのタイプが記述される。システム構成例ＤＢ５４４は、サブシステムのタイプを検索キーとして、所望のサブシステムのシステム展開パターン５４４１を検索できるようにデータベース化されている。

【００３５】

運用環境事例ＤＢ５４５には、過去にシステムセキュリティ仕様書が作成された情報ネットワークシステムの各サブシステムの運用環境パターンが運用環境事例として登録されている。ここで、運用環境パターンとは、サブシステムのシステム展開パターンに、該システムの各コンポーネントに適用した運用方針や前提条件が記述されて構成されたものである。

【００３６】

図７は、運用環境事例ＤＢ５４５の登録例を示す図である。図示するように、運用環境パターン５４５１は、図６に示すシステム展開パターン５４４１において、サブシステムおよびコンポーネント各々の記述領域に、対応する構成要素に適用した運用方針や前提条件を記述するための領域（２つのタグ＜運用＞、＜/運用＞で囲まれた領域）５４５２が設けられて構成されている。運用環境事例ＤＢ５４５も、システム構成例ＤＢ５４４と同様に、サブシステムのタイプを検索キーとして、所望のサブシステムの運用環境パターン５４５１を検索できるようにデータベース化されている。

【００３７】

また、メモリ５５には、ＣＰＵ５１がメモリ５５にロードされたセキュリティ仕様書作成支援ＰＧ５４２を実行することにより、運用環境事例ＤＢ５４５から読み出した運用環境事例を一時格納するための運用環境事例格納領域５５１、システム構成事例ＤＢ５４４から読み出したシステム構成事例を一時格納するためのシステム構成事例格納領域５５２、セキュリティ仕様書事例ＤＢ５４３から読

み出したセキュリティ仕様書事例を一時格納するためのセキュリティ仕様書事例格納領域５５３、設計対象システムの定義情報を一時格納するための設計対象システム定義情報格納領域５５４、および、設計対象システムのセキュリティ仕様書原案を一時格納するためのセキュリティ仕様書原案格納領域５５５が、それぞれ形成される。

【００３８】

図８は、本実施形態のセキュリティ仕様書作成支援装置１１の動作フローを説明するための図である。

【００３９】

まず、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介して、設計対象システムの階層構造を示す定義情報を、ユーザより対話的に受付ける。そして、設計対象システムの定義情報を設計対象システム定義情報格納領域５５４に格納する（Ｓ７１１）。

【００４０】

次に、セキュリティ仕様書選定ＰＧ５４２２は、設計対象システム定義情報格納領域５５４に格納された、設計対象システムの定義情報により特定されるコンポーネントの中からコンポーネントを１つ抽出し、これを注目コンポーネントとする。そして、注目コンポーネントの定義情報（カテゴリ５４３１、タイプ５４３２）と適合するセキュリティ仕様書の事例を検出する。そして、ユーザの指示に従い、検出した事例の中から、注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例（例えば所属ドメインの運用方針と適合するセキュリティ仕様書の事例）を選択する（Ｓ７１２）。

【００４１】

次に、セキュリティ仕様書選定ＰＧ５４２２は、注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例を選定できた場合（Ｓ７１３でＹｅｓ）、これをセキュリティ仕様書事例ＤＢ５４３から読み出してセキュリティ仕様書事例格納領域５５３に格納する。次に、セキュリティ仕様書原案作成ＰＧ５４２３は、セキュリティ仕様書事例格納領域５５３に格納されたセキュリティ仕様書の事例を、端末入手力装置５２を介して、ユーザに提示し、その修正を受付ける

。これにより、注目コンポーネントに対するセキュリティ仕様書原案が作成される。そして、ユーザの登録指示に従い、注目コンポーネントに対するセキュリティ仕様書原案を、それが既存のセキュリティ仕様書の事例をベースにしていることが分かるようにして、セキュリティ仕様書原案格納領域５５５に格納する（Ｓ７１４）。それからＳ７１６に移行する。

【００４２】

一方、セキュリティ仕様書選定ＰＧ５４２２が注目コンポーネントに対して再利用可能なセキュリティ仕様書の事例を選定できなかった場合（Ｓ７１３でＮｏ）、セキュリティ仕様書原案作成ＰＧ５４２３は、端末入手力装置５２を介してユーザより、注目コンポーネントに対するセキュリティ仕様書原案を新規に受け付ける。そして、ユーザの登録指示に従い、注目コンポーネントに対するセキュリティ仕様書原案を、それが新規作成されたものであることが分かるようにして、セキュリティ仕様書原案格納領域５５５に格納する（Ｓ７１５）。それからＳ７１６に移行する。

【００４３】

次に、Ｓ７１６において、セキュリティ仕様書選定ＰＧ５４２２は、設計対象システムの定義情報により特定されるコンポーネント中に、注目コンポーネントとして未抽出のコンポーネントがあるか否かを調べる。そして、未抽出のコンポーネントがあるならば（Ｓ７１６でＮｏ）、Ｓ７１２に戻る。

【００４４】

一方、設計対象システムの定義情報により特定される全てのコンポーネントが注目コンポーネントとして抽出された場合、つまり、設計対象システムの定義情報により特定される全てのコンポーネントに対するセキュリティ仕様書原案がセキュリティ仕様書原案格納領域５５５に格納された場合（Ｓ７１６でＹｅｓ）、セキュリティ仕様書原案作成ＰＧ５４２３は、予め用意してあるセキュリティ仕様書の雛形に、各コンポーネントのセキュリティ仕様書原案の内容を反映させて、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する（Ｓ７１７）。

【００４５】

具体的には、ＩＳＯ１５４０８準拠セキュリティ仕様書のある目次について、当該目次における記述内容を、各コンポーネントのセキュリティ仕様書原案から抽出し、これらを予め用意してあるセキュリティ仕様書の雛形における当該目次の内容記述部分に追加する。この際、追加した記述内容の参照元（コンポーネントのセキュリティ仕様書原案）へのリンク情報を追加する。以上の処理を、ＩＳＯ１５４０８準拠セキュリティ仕様書の全ての目次に対して繰り返し行うことにより、各コンポーネントのセキュリティ仕様書原案の内容が反映された、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する。

【００４６】

次に、セキュリティ仕様書原案作成ＰＧ５４２３は、自動作成した設計対象システムに対するコンポジットセキュリティ仕様書原案を、端末入手力装置５２を介して、ユーザに提示し、その修正を受付ける。そして、ユーザの登録指示に従い、設計対象システムに対するコンポジットセキュリティ仕様書原案を、セキュリティ仕様書原案格納領域５５５に格納する（Ｓ７１８）。

【００４７】

セキュリティ仕様書原案格納領域５５５に格納されたコンポジットセキュリティ仕様書原案および各コンポーネントのセキュリティ仕様書原案は、設計対象システムのシステムセキュリティ仕様書原案として、端末入出力装置５２を介してユーザに提示されたり、外部記憶装置５４や可搬記憶媒体入出力装置５９に装着された可搬記憶媒体５９１に記憶されたり、ネットワークＩＦ装置５８を介してネットワークへ送信されたりする。

【００４８】

図９は、図８のＳ７１１での処理（設計対象システムの定義情報の受付・登録）の詳細なフローを示す図である。

【００４９】

先ず、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、設計対象システムを構成する各ドメインの設定を受付ける（Ｓ７１１１）。ユーザは、例えば地理的条件や会社の組織構成などに基づいて、設計対象システムを、共通の運用方針が適用されるサブシステムのグループである複数のドメ

インに分割する。そして、各ドメインの設定をセキュリティ仕様書作成支援装置１１に入力する。

【００５０】

次に、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、上記のＳ７１１１で受付けた各ドメインについて、運用方針を含むドメイン固有情報および他ドメインとのインターフェースに関するドメイン間対応情報を、ドメインの定義情報として受付ける（Ｓ７１１２）。

【００５１】

次に、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、ドメイン各々について当該ドメインに属するサブシステムの設定を受付ける（Ｓ７１１３）。ユーザは、ドメイン各々について、当該ドメインに属するＩＴ製品、ネットワークインフラ等の個々のサブシステムを特定し、特定したサブシステム各々の設定をセキュリティ仕様書作成支援装置１１に入力する。

【００５２】

次に、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、上記のＳ７１１３で受付けた各サブシステムについて、サブシステム固有情報および他サブシステムとのインターフェースに関するサブシステム間対応情報を、サブシステムの定義情報として受付ける（Ｓ７１１４）。

【００５３】

次に、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、サブシステム各々について当該サブシステムを構成するコンポーネントの設定を受付ける（Ｓ７１１５）。ユーザは、サブシステム各々について、当該サブシステムを構成するソフト部品、ハード部品等の個々のコンポーネントを特定し、特定したコンポーネント各々の設定をセキュリティ仕様書作成支援装置１１に入力する。

【００５４】

次に、システム構成定義ＰＧ５４２１は、端末入手力装置５２を介してユーザより、上記のＳ７１１５で受付けた各コンポーネントについて、コンポーネント固有情報および他コンポーネントとのインターフェースに関するコンポーネント

間対応情報を、コンポーネントの定義情報として受付ける（Ｓ７１１６）。

【００５５】

以上のようにして、ドメイン、サブシステムおよびコンポーネントの定義情報を受付けたならば、システム構成定義ＰＧ５４２１は、これらの定義情報を設計対象システムの階層構造を示す定義情報として、設計対象システム定義情報格納領域５５４に格納する。

【００５６】

図１０は、システム構成定義ＰＧ５４２１が表示装置５６に表示する作業画面のメニューバーの一例を示す図である。先ず、図１０を用いて、図８のＳ７１１（設計対象システムの定義情報の受付、図９に示すフロー）における操作手順と画面構成を説明する。

【００５７】

システム構成定義ＰＧ５４２１は、図１０（Ａ）に示すように、初期画面として仕様書編集画面９１を表示する。入力装置５７を介してカーソル（不図示）が操作されて、ユーザにより、メニューバーの項目「ツール」９１１から項目「ＴＯＥ定義支援」９１１１が選択されると、設計対象システム定義情報格納領域５５４に格納されている設計対象システムの定義情報によって特定されるシステム展開ツリー（設計対象システムの階層構造）を表示するＴＯＥ定義画面９２を、端末入出力装置５２を介して表示装置５６に表示する。なお、このＴＯＥ定義画面９２を閉じる場合、図１０（Ｂ）に示すように、ユーザはメニューバーの項目「ファイル」９２１から項目「閉じる」９２１１を選択すればよい。

【００５８】

図１１は、システム構成定義ＰＧ５４２１が表示装置５６に表示するＴＯＥ定義画面９２の一例を示している。この例では、図８に示すフローが実行されて、図２に示す勤休管理システムの定義情報が設計対象システム定義情報格納領域５５４に格納され、また、勤休管理システムのシステムセキュリティ仕様書原案がセキュリティ仕様書原案格納領域５５５に格納された状態にて、項目「ＴＯＥ定義支援」９１１１が選択された場合を示している。

【００５９】

システム構成定義ＰＧ５４２１は、表示枠９２４に、設計対象システム定義情報格納領域５５４に格納されている設計対象システムの定義情報により特定されるシステム展開ツリーを表示する。なお、設計対象システム定義情報格納領域５５４に設計対象システムの定義情報が格納されていない状態、つまり、これから設計対象システムの定義情報を受付ける状態では、表示枠９２４には何も表示されない。

【００６０】

図１１において、四角マークのノード９２４１～９２４３がドメインである。図２に示す勤休管理システムの場合、「本社拠点区域」ドメイン９２４１、「支社拠点区域」ドメイン９２４２、および、「拠点間ネットワーク」ドメイン９２４３の３つのドメインに分けることができる。なお、ドメインの追加は、図１０（Ｃ）に示すように、入力装置５７を介してカーソル（不図示）を操作し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「要素の追加」９２２２を選択し、さらに項目「ドメイン」９２２３を選択することで行う。これにより、システム構成定義ＰＧ５４２１は、「ＴＯＥ」ノード９２４０に接続する四角マークの新たなノードを追加表示する（図９のＳ７１１１）。

【００６１】

また、図１１において、三角マークのノード９２４４、９２４５がサブシステムである。図２に示す勤休管理システムの場合、例えば「本社拠点区域」ドメイン９２４１には、「一般利用者端末」サブシステム９２４４および「勤休管理サーバ」サブシステム９２４５が属している。なお、サブシステムの追加は、図１０（Ｃ）に示すように、入力装置５７を介してカーソル（不図示）を操作し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「要素の追加」９２２２を選択し、さらに項目「サブシステム」９２２４を選択すると共に、所望のドメインのノードを指定することで行う。これにより、システム構成定義ＰＧ５４２１は、所望のドメインのノードに接続する三角マークの新たなノードを追加表示する（図９のＳ７１１３）。

【００６２】

また、図１１において、丸マークのノード９２４６～９２５６がコンポーネン

トである。図２に示す勤休管理システムの場合、例えば「一般利用者端末」サブシステム９２４４には、「アプリ層」コンポーネント９２４６、「勤休入力用ブラウザ」コンポーネント９２４９、「通知受信用メーラ」コンポーネント９２５０、「ＯＳ層」コンポーネント９２４７、「端末ＯＳ」９２５１、「ハードウエア層」コンポーネント９２４８、「ＡＴ互換ハードウエア」コンポーネント９２５２、「ネットワークカード」９２５３が属している。なお、コンポーネントの追加は、図１０（Ｃ）に示すように、入力装置５７を介してカーソル（不図示）を操作し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「要素の追加」９２２２を選択し、さらに項目「コンポーネント」９２２５を選択すると共に、所望のサブシステムあるいはコンポーネントのノードを指定することで行う。これにより、システム構成定義ＰＧ５４２１は、所望のサブシステムあるいはコンポーネントのノードに接続する丸マークの新たなノードを追加表示する（図９のＳ７１１５）。

【００６３】

ここで、コンポーネントのノードを、サブシステムのノードみならず、他のコンポーネントのノードにも接続できるようにすることで、同一レイヤのコンポーネントを水平方向に展開する方法で表示することができる。これにより、ネットワーク接続関係にあるような水平分散する要素群（ドメイン、サブシステム）と、ＩＴ製品のレイヤ構造のような垂直展開する要素群（コンポーネント）との両方を識別することができる。

【００６４】

また、システム構成定義ＰＧ５４２１は、表示枠９２６に、表示枠９２４に表示されているシステム展開ツリーから、ユーザがカーソル（不図示）を操作して選択したノードの定義情報を表示する。図１１に示す例では、「勤休入力用ブラウザ」コンポーネント９２４９が選択され、その定義情報が表示枠９２６に表示されている。なお、設計対象システム定義情報格納領域５５４に、選択されたノードの定義情報が格納されていない状態、つまり、これから当該ノードの定義情報を受付ける状態では、表示枠９２６には何も表示されない。

【００６５】

また、図１０（Ｃ）に示すように、ユーザがカーソル（不図示）を操作して表示枠９２４に表示されているドメインのノードを指定し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「定義情報の設定」９２２１を選択すると、システム構成定義ＰＧ５４２１は、設計対象システム定義情報格納領域５５４に格納されている当該ドメインの定義情報を表示すると共に当該ドメインの定義情報の修正を受付けるためのドメイン定義画面９３を、端末入出力装置５２を介して表示装置５６に表示する。

【００６６】

図１２は、システム構成定義ＰＧ５４２１が表示装置５６に表示するドメイン定義画面９３の一例を示している。この例では、図１１において「本社拠点区域」ドメイン９２４１が指定された場合であって、「本社拠点区域」ドメイン９２４１の定義情報が既に設計対象システム定義情報格納領域５５４に格納されている場合の表示を示している。

【００６７】

図示するように、ドメイン定義画面９３は、ドメインの固有情報の入力欄として、ドメイン名称、ドメインの詳細説明であるドメイン記述、および、ドメイン内の保護対象資産の入力欄９３２～９３４を有する。また、ドメイン間対応情報の入力欄として、対象ドメインとのインターフェースを有する相手ドメインを設定するための設定欄９３５を有する。設定欄９３５は、設計対象システムを構成するドメインを相手ドメイン候補として一覧表示する相手候補表示欄９３５１と、この相手候補表示欄９３５１から選択された相手ドメインを表示する相手表示欄９３５２とを有する。また、対象ドメインに適用する運用方針、前提条件等の運用環境を入力する入力欄９３６を有する。

【００６８】

なお、設計対象システム定義情報格納領域５５４に、指定されたドメインの定義情報が格納されていない状態、つまり、これから当該ドメインの定義情報を受付ける状態では、各入力欄９３２～９３４、９３６および相手表示欄９３５２には何も表示されない。

【００６９】

端末入出力装置５２を介してユーザが各入力欄９３２～９３４、９３６に適切な情報を入力すると共に、相手ドメインを選択して相手表示欄９３５２に相手ドメインを表示させ、ＯＫボタン９３７を選択すると、システム構成定義ＰＧ５４２１は、各入力欄９３２～９３４、９３６および相手表示欄９３５２に表示されているドメインの固有情報、ドメイン間対応情報および運用環境情報を、当該ドメインの定義情報として、設計対象システム定義情報格納領域５５４に登録あるいは更新する（図９のＳ７１１２）。

【００７０】

また、図１０（Ｃ）に示すように、ユーザがカーソル（不図示）を操作して表示枠９２４に表示されているサブシステムのノードを指定し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「定義情報の設定」９２２１を選択すると、システム構成定義ＰＧ５４２１は、設計対象システム定義情報格納領域５５４に格納されている当該サブシステムの定義情報を表示すると共に当該サブシステムの定義情報の修正を受付けるためのサブシステム定義画面９４を、端末入出力装置５２を介して表示装置５６に表示する。

【００７１】

図１３は、システム構成定義ＰＧ５４２１が表示装置５６に表示するサブシステム定義画面９４の一例を示している。この例では、図１１において「一般利用者端末」サブシステム９２４４が指定された場合であって、「一般利用者端末」サブシステム９２４４の定義情報が既に設計対象システム定義情報格納領域５５４に格納されている場合の表示を示している。

【００７２】

図示するように、サブシステム定義画面９４は、サブシステムの固有情報の入力欄として、装置種別を示すサブシステムタイプ、サブシステム名称、サブシステムの詳細説明であるサブシステム記述、および、サブシステム内の保護対象資産の入力欄９４１～９３４を有する。また、サブシステム間対応情報の入力欄として、対象サブシステムとのインターフェースを有する相手サブシステムを設定するための設定欄９４５を有する。設定欄９４５は、同じドメインに属するサブシステムおよびネットワークを介して接続関係にある他ドメイン（このドメイン

は前記同じドメインのドメイン間対応情報により特定できる）のサブシステムを相手サブシステム候補として一覧表示する相手候補表示欄９４５１と、この相手候補表示欄９４５１から選択された相手サブシステムを表示する相手表示欄９４５２とを有する。また、対象サブシステムに適用する運用方針、前提条件等の運用環境を入力する入力欄９４６を有する。

【００７３】

なお、設計対象システム定義情報格納領域５５４に、指定されたサブシステムの定義情報が格納されていない状態、つまり、これから当該サブシステムの定義情報を受付ける状態では、各入力欄９４１～９４４、９４６および相手表示欄９４５２には何も表示されない。

【００７４】

端末入出力装置５２を介してユーザが各入力欄９４１～９４４、９４６に適切な情報を入力すると共に、相手サブシステムを選択して相手表示欄９４５２に相手サブシステムを表示させ、ＯＫボタン９４７を選択すると、システム構成定義ＰＧ５４２１は、各入力欄９４１～９４４、９４６および相手表示欄９４５２に表示されているサブシステムの固有情報、サブシステム間対応情報および運用環境情報を、当該サブシステムの定義情報として、設計対象システム定義情報格納領域５５４に登録あるいは更新する（図９のＳ７１１４）。

【００７５】

ここで、サブシステムタイプの入力欄９４１にサブシステムタイプが入力されている場合、システム構成定義ＰＧ５４２１は、このタイプを検索キーとして、システム構成事例ＤＢ５４４からサブシステムのシステム展開パターン５４４１を検索してもよい。そして、システム展開パターン５４４１を検出できたならば、検出したシステム展開パターン５４４２により特定される各コンポーネントを、対象サブシステムを構成するコンポーネントとして、図１１に示すＴＯＥ定義画面９２の表示枠９２４に追加表示し、これらを対象サブシステムのノードに接続するようにしてもよい。例えば、入力欄９４１にサブシステムタイプ「ＩＴ機器」が入力され、ＯＫボタン９４７が選択されると、システム構成定義ＰＧ５４２１は、サブシステムタイプ「ＩＴ機器」のシステム展開パターン５４４１を検

索し、該パターン５４４１により特定される各コンポーネント（図６に示す例では、アプリケーション層、ミドルウエア層、ＯＳ層、ハードウエア層）を、対象サブシステムを構成するコンポーネントとして設定する。そして、図１１に示すＴＯＥ定義画面９２の表示枠９２４に、対象サブシステムのノードに接続された各コンポーネントのノードを追加表示する。このようにすることで、対象サブシステムを構成するコンポーネントの追加を自動化することができる。

【００７６】

また、図１０（Ｃ）に示すように、ユーザがカーソル（不図示）を操作して表示枠９２４に表示されているコンポーネントのノードを指定し、ＴＯＥ定義画面９２において、メニューバーの項目「編集」９２２から項目「定義情報の設定」９２２１を選択すると、システム構成定義ＰＧ５４２１は、設計対象システム定義情報格納領域５５４に格納されている当該コンポーネントの定義情報を表示すると共に当該コンポーネントの定義情報の修正を受付けるためのコンポーネント定義画面９５を、端末入出力装置５２を介して表示装置５６に表示する。

【００７７】

図１４は、システム構成定義ＰＧ５４２１が表示装置５６に表示するコンポーネント定義画面９５の一例を示している。この例では、図１１において「勤休入力用ブラウザ」コンポーネント９２４９が指定された場合であって、「勤休入力用ブラウザ」コンポーネント９２４９の定義情報が既に設計対象システム定義情報格納領域５５４に格納されている場合の表示を示している。

【００７８】

図示するように、コンポーネント定義画面９５は、コンポーネントの固有情報の入力欄として、部品種別を示すコンポーネントタイプ、コンポーネント名称、コンポーネントの詳細説明であるコンポーネント記述、コンポーネント内の保護対象資産、コンポーネントの特徴情報（カテゴリおよびタイプ）、目標とするＥＡＬ（Evaluation Assurance Level）、および、準拠すべきセキュリティ仕様書名または使用すべき既存製品名の入力欄９５１～９５４、９５８、９６０、９６１を有する。ここで、コンポーネントの特徴情報（カテゴリおよびタイプ）は、セキュリティ仕様書事例ＤＢ５４３からセキュリティ仕様書の事例を検索するた

めの検索キーとして用いられる。

【００７９】

また、コンポーネント定義画面９５は、コンポーネント間対応情報の入力欄として、対象コンポーネントとのインターフェースを有する相手コンポーネントを設定するための設定欄９５５と、対象コンポーネントと機能的に関係する他のコンポーネントを設定するための設定欄９５９とを有する。設定欄９５５は、同じサブシステムに属するコンポーネントおよびネットワークを介して接続関係にある他サブシステム（このサブシステムは前記同じサブシステムのサブシステム間対応情報により特定できる）に属するコンポーネントを相手コンポーネント候補として一覧表示する相手候補表示欄９５５１と、この相手候補表示欄９５５１から選択された相手コンポーネントを表示する相手表示欄９５５２と、を有する。設定欄９５９も、同様に、同じサブシステムに属するコンポーネントおよびネットワークを介して接続関係にある他サブシステムに属するコンポーネントを関連コンポーネント候補として一覧表示する関連候補表示欄９５９１と、この関連候補表示欄９５９１から選択された関連コンポーネントを表示する関連表示欄９５９２と、を有する。

【００８０】

また、コンポーネント定義画面９５は、対象コンポーネントに適用する運用方針、前提条件等の運用環境を入力する入力欄９５６を有する。なお、設計対象システム定義情報格納領域５５４に、指定されたコンポーネントの定義情報が格納されていない状態、つまり、これから当該コンポーネントの定義情報を受付ける状態では、各入力欄９５１～９５４、９５６、９５８、９６０、９６１、相手表示欄９５５２および関連表示欄９５９２には何も表示されない。

【００８１】

端末入出力装置５２を介してユーザが各入力欄９５１～９５４、９５６、９５８、９６０、９６１に適切な情報を入力すると共に、相手コンポーネント、関連コンポーネントを選択して相手表示欄９５５２、関連表示欄９５９２に相手コンポーネント、関連コンポーネントを表示させ、ＯＫボタン９５７を選択すると、システム構成定義ＰＧ５４２１は、各入力欄９５１～９５４、９５６、９５８、

９６０、９６１、相手表示欄９５５２および関連表示欄９５９２に表示されているコンポーネントの固有情報、コンポーネント間対応情報および運用環境情報を、当該コンポーネントの定義情報として、設計対象システム定義情報格納領域５５４に登録あるいは更新する（図９のＳ７１１６）。

【００８２】

ここで、コンポーネントタイプの入力欄９５１にコンポーネントタイプが入力された場合、システム構成定義ＰＧ５４２１は、対象コンポーネントが属するサブシステムの定義情報に含まれているサブシステムタイプを検索キーとして、運用環境事例ＤＢ５４５からサブシステムの運用環境パターン５４５１を検索し、さらに、入力欄９５１に入力されたコンポーネントタイプを検索キーとして、検出した運用環境パターン５４５１から対象コンポーネントの運用環境情報を抽出してもよい。そして、抽出した運用環境情報を、運用環境の入力欄９５６の初期値として表示してもよい。例えば、システム構成定義ＰＧ５４２１は、対象コンポーネントが属するサブシステムのタイプが「ＩＴ機器」の場合、サブシステムタイプ「ＩＴ機器」の運用環境パターン５４５１を検索する。そして、入力欄９５１にコンポーネントタイプ「アプリケーション層」が入力されると、検出した運用環境パターン５４５１からコンポーネントタイプ「アプリケーション層」の運用環境情報を抽出し、これを入力欄９５６に初期表示する。このようにすることで、対象コンポーネントの運用環境情報の作成負担を軽減することができる。

【００８３】

以上のようにして、図８のＳ７１１（図９に示すフロー）が行われ、設計対象システムの定義情報が設計対象システム定義情報格納領域５５４に登録・更新される。

【００８４】

次に、図１０を用いて、図８のＳ７１２～Ｓ７１６（各コンポーネントのセキュリティ仕様原案の作成・登録）における操作手順と画面構成を説明する。

【００８５】

図１０（Ｄ）に示すように、ユーザがカーソル（不図示）を操作し、ＴＯＥ定義画面９２において、メニューバーの項目「ツール」９２３から項目「コンポー

ネント仕様書原案作成」９２３１を選択すると、セキュリティ仕様書選定ＰＧ５４２２は、設計対象システムの定義情報により特定されるコンポーネント各々を注目コンポーネントとして、図８のＳ７１２～Ｓ７１６を実行する。

【００８６】

図１５は、セキュリティ仕様書選定ＰＧ５４２２が表示装置５６に表示する再利用可能事例画面９６の一例を示している。ここで、表示枠９６１には、注目コンポーネントの特徴情報（カテゴリ、タイプ）９５８を検索キーとして、セキュリティ仕様書事例ＤＢ５４３から検索した既存のセキュリティ仕様書のタイトルが表示される。表示枠９６３には、ユーザがカーソル（不図示）を操作して表示枠９６１の中から選択したタイトルのセキュリティ仕様書の内容が表示される。ユーザは、表示枠９６３に表示されたセキュリティ仕様書の内容を参照することで、注目コンポーネントの定義情報に記載された各種情報（目標ＥＡＬ、運用環境、所属サブシステム）と当該セキュリティ仕様書との整合性等を検証することができる。これにより、当該セキュリティ仕様書を注目コンポーネントに再利用できるか否かの判断を適切に行うことが可能となる。また、表示枠９６２は、ユーザがカーソル（不図示）を操作し、再利用するセキュリティ仕様書として、表示枠９６１の中から選択したタイトルのセキュリティ仕様書のタイトルが表示される。表示枠９６２にタイトルが表示されている状態でＯＫボタン９６４が選択されると、セキュリティ仕様書選定ＰＧ５４２２は、このタイトルを持つセキュリティ仕様書を、注目コンポーネントに対して再利用するセキュリティ仕様書に決定する（図８のＳ７１４）。

【００８７】

図１６は、セキュリティ仕様書原案作成ＰＧ５４２３が表示装置５６に表示するセキュリティ仕様書作成・編集画面９７の一例を示している。セキュリティ仕様書原案作成ＰＧ５４２３は、セキュリティ仕様書選定ＰＧ５４２２により注目コンポーネントについて再利用するセキュリティ仕様書の事例が選定されたならば、このセキュリティ仕様書の内容を、セキュリティ仕様書作成・編集画面９７の注目コンポーネントのタグ９７１が付された編集領域９７２に表示する。そして、端末入出力装置５２を介してユーザより、セキュリティ仕様書の編集を受付

ける。それから、ユーザより登録指示を受付けたならば、編集領域９７２に表示されているセキュリティ仕様書を注目コンポーネントのセキュリティ仕様書原案として、再利用したセキュリティ仕様書原案の情報（タイトル名など）と共に、セキュリティ仕様書原案格納領域５５５に格納する。なお、注目コンポーネントについて再利用するセキュリティ仕様書の事例が選定されなかった場合、初期状態では注目コンポーネントのタグ９７１が付された編集領域９７２に何も表示されない。したがって、ユーザは、注目コンポーネントのタグ９７１が付された編集領域９７２に、注目コンポーネントのセキュリティ仕様書原案を最初から記入する必要がある（図８のＳ７１４、７１５）。

【００８８】

以上のようにして、図８のＳ７１２～Ｓ７１６が行われ、設計対象システムの各コンポーネントのセキュリティ仕様書原案がセキュリティ仕様書原案格納領域５５５に登録・更新される。

【００８９】

次に、図１０を用いて、図８のＳ７１７、Ｓ７１８（設計対象システムのコンポジットセキュリティ仕様書原案の作成・登録）における操作手順と画面構成を説明する。

【００９０】

図１０（Ｄ）に示すように、ユーザがカーソル（不図示）を操作し、ＴＯＥ定義画面９２において、メニューバーの項目「ツール」９２３から項目「コンポジット仕様書原案作成」９２３２を選択すると、セキュリティ仕様書原案作成ＰＧ５４２３は、予め用意してあるセキュリティ仕様書の雛形に、セキュリティ仕様書原案格納領域５５５に格納されている各コンポーネントのセキュリティ仕様書原案の内容を反映させて、設計対象システムに対するコンポジットセキュリティ仕様書原案を自動作成する（図８のＳ７１７）。

【００９１】

図１７は、セキュリティ仕様書原案作成ＰＧ５４２３が表示装置５６に表示するセキュリティ仕様書作成・編集画面９７の一例を示している。図１７に示すセキュリティ仕様書作成・編集画面９７は、図１６に示すセキュリティ仕様書作成

・編集画面９７において、設計対象システムのタグ９７３が付された編集領域９７４に、セキュリティ仕様書原案作成ＰＧ５４２３が自動生成したコンポジットセキュリティ仕様書原案が表示されたものである。セキュリティ仕様書原案作成ＰＧ５４２３は、端末入出力装置５２を介してユーザより、編集領域９７４に表示したコンポジットセキュリティ仕様書の編集を受付ける。それから、ユーザより登録指示を受付けたならば、編集領域９７４に表示されているコンポジットセキュリティ仕様書をセキュリティ仕様書原案格納領域５５５に格納する。これにより、セキュリティ仕様書原案格納領域５５５に、設計対象システムのシステムセキュリティ仕様書原案が登録される（図８のＳ７１８）。

【００９２】

上述したように、図１１は、設計対象システムの定義情報が設計対象システム定義情報格納領域５５４に格納され、また、システムセキュリティ仕様書原案がセキュリティ仕様書原案格納領域５５５に格納された状態にて、項目「ＴＯＥ定義支援」９１１１が選択された場合に表示されるＴＯＥ定義画面９２を示している。各コンポーネントのノードを、セキュリティ仕様書原案の作成に既存のセキュリティ仕様書を利用したか否かが識別できるように表示している。これは、セキュリティ仕様書原案格納領域５５５に格納されているコンポーネントのセキュリティ仕様書原案に、再利用したセキュリティ仕様書原案の情報（タイトル名など）が付されているか否かを調べることで判断することができる。既存のセキュリティ仕様書を利用したコンポーネントのノード９２４９、９２４７、９２５１、９２５２、９２５４～９２５６は、黒く塗りつぶした丸マークで表示し、既存のセキュリティ仕様書を利用していないコンポーネントのノード９２４６、９２４８、９２５０、９２５３は、白抜きの丸マークで表示している。このようにすることで、ユーザはコンポーネントの評価の有無を把握することができる。

【００９３】

また、図１１において、サブシステムに属する全てのコンポーネントが既存のセキュリティ仕様書を利用している場合、当該サブシステムのノードを、そのことが識別できるように表示している。自身に属する全てのコンポーネントが既存のセキュリティ仕様書を利用しているサブシステム「勤休管理サーバ」のノード

９２４５は、黒く塗りつぶした三角マークで表示し、そうでないサブシステム「一般利用者端末」のノード９２４４は、白抜きの三角マークで表示している。このようにすることで、ユーザはサブシステムの評価の有無を把握することができる。ドメインも同様である。

【００９４】

また、図１１に示すＴＯＥ定義画面９２において、表示枠９２５は、表示枠９２４に表示されているシステム展開ツリーから、ユーザがカーソル（不図示）を操作して選択したノードのコンポーネントが、既存のセキュリティ仕様書を再利用している場合に、その既存のセキュリティ仕様書の情報（タイトル名など）が表示される。

【００９５】

以上、本発明の一実施形態について説明した。

【００９６】

本実施形態によれば、設計対象システムを構成する各コンポーネントの定義情報をユーザより受付ける。次に、コンポーネント各々について、セキュリティ仕様書事例ＤＢ５４３に再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。それから、予め用意してあるセキュリティ仕様書の雛形に、特定したセキュリティ仕様書各々の内容を反映して、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動生成し、ユーザに提示する。そして、ユーザよりコンポジットセキュリティ仕様書の原案の修正を受付ける。このようにすることで、専門知識・技術やノウハウを持もたないユーザが設計対象システムのセキュリティ仕様書原案を作成することを支援することができる。

【００９７】

本実施形態は、より具体的には以下の効果を有する。

【００９８】

（１）設計対象システムに対するコンポジットセキュリティ仕様書原案を自動生成し、差分情報のみを追加、修正することにより、セキュリティ仕様書の作成工数を削減することができる。

【００９９】

（２）各コンポーネントに対して既存（認証済み）のセキュリティ仕様書を再利用することにより、リスク分析等の専門的な技術と知識を必要とする作業を省くことができる。これにより、セキュリティ設計工数の大部分を占める分析作業を削減でき、複数の要素から構成される情報ネットワークシステムにおいて膨大となりがちな設計工数を削減できる。

【０１００】

（３）各コンポーネントに対して既存（認証済み）のセキュリティ仕様書を再利用することにより、一定品質を確保したセキュリティ仕様書原案の作成が可能となり、複数の要素から構成されるため膨大となりやすい情報ネットワークシステムの評価コストを削減できる。

【０１０１】

（４）システム要件等に基づいて設計対象システムを構成要素に分解、定義することができ、このため、システム構成と矛盾しないシステムセキュリティ設計が可能となる。

【０１０２】

（５）顧客先でシステムセキュリティ設計コンサルテーションを行う場合等に、可搬記憶媒体に格納したセキュリティ仕様書事例ＤＢ５４４を利用することで、高品質なコンサルテーションサービスをすばやく提供することができる。

【０１０３】

なお、本発明は上記の実施形態に限定されるものではなく、その要旨の範囲内で数々の変形が可能である。

【０１０４】

例えば、上記の実施形態において、セキュリティ仕様書原案作成ＰＧ５４２３に、コンポジットセキュリティ仕様書原案を、設計対象システムのみならず、ドメイン単位やサブシステム単位でも自動作成させるようにしてもよい。ドメインあるいはサブシステムのコンポジットセキュリティ仕様書原案の自動作成は、予め用意してあるセキュリティ仕様書の雛形に、対象ドメインあるいはサブシステムに属する各コンポーネントのセキュリティ仕様書原案の内容を反映するように

すればよい。そして、自動作成されたコンポジットセキュリティ仕様書原案をユーザに提示して修正を受付けるようにすればよい。

【０１０５】

また、ドメインあるいはサブシステムのコンポジットセキュリティ仕様書原案から作成したドメインあるいはサブシステムのコンポジットセキュリティ仕様書を、コンポーネントのセキュリティ仕様書と同様、セキュリティ仕様書事例ＤＢ５４３に登録するようにしてもよい。サブシステムのコンポジットセキュリティ仕様書を、サブシステムタイプ（図１３の入力欄９４１に入力される情報）、および、サブシステムを構成する各コンポーネントの特徴情報（図１４の入力欄９５８に入力される情報）をキーとして検索できるようにデータベース化する。また、ドメインのコンポジットセキュリティ仕様書を、ドメインを構成する各サブシステムのサブシステムタイプ、および、サブシステム各々を構成する各コンポーネントの特徴情報をキーとして検索できるようにデータベース化する。

【０１０６】

このようにすることで、設計対象システム定義情報格納領域５５４に格納された設計対象システムのシステム定義情報から、ドメインあるいはサブシステムの各々について、再利用可能なドメインあるいはサブシステムのコンポジットセキュリティ仕様書の事例を検索することができる。そして、ドメインあるいはサブシステムに対して検出されたコンポジットセキュリティ仕様書を、当該ドメインあるいは当該サブシステムのコンポジットセキュリティ仕様書原案とし、当該ドメインあるいは当該サブシステム以外のドメイン、サブシステムに属する各コンポーネントのセキュリティ仕様書原案と同様に、コンポジットセキュリティ仕様書の雛形に反映させることにより、同一または類似の部分構成を備える大規模システムのセキュリティ仕様書の作成工数を削減できる。

【０１０７】

また、上記の実施形態において、ＤＢ５４３～５４５は、セキュリティ仕様書作成支援装置１１にローカル接続されている必要はない。ネットワーク上に配置するようにしても構わない。図１８は、セキュリティ仕様書作成支援装置１１の変形例を示す図である。

【０１０８】

図１８に示すセキュリティ仕様書作成装置１１は、例えばセキュリティ設計支援サービス企業やベンダ企業やＳＩ（System Integrater）企業等に設置されており、ＬＡＮ、ＷＡＮ等のネットワーク１５を介して、セキュリティ仕様書の国際/国内登録機関や、官公庁の調達要件書を作成し管理している公的機関や、業界標準を規定する業界団体や、セキュリティ情報を提供することで利益を得ている企業等のＤＢ管理装置１５０と接続されている。また、ＤＢ管理装置１５０には、セキュリティ仕様書事例ＤＢ５４３が接続されている。

【０１０９】

このセキュリティ仕様書作成支援装置１１において、セキュリティ仕様書選定ＰＧ５４２２は、ネットワークＩＦ装置５８およびＤＢ管理装置１５０を介して、セキュリティ仕様書事例ＤＢ５４３にアクセスし、再利用可能なセキュリティ仕様書の事例を入手する。このようにすることで、ネットワーク１５上に分散する多種多様な既存のセキュリティ仕様書の中から設計対象に最適なものを効率的に選定したり、官公庁や業界団体が指定する最新のセキュリティ仕様書を直接入手したりすることが可能となり、より高品質かつ効率的な設計が可能となる。

【０１１０】

【発明の効果】

以上説明したように、本発明によれば、複数のＩＴ製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援することができる。

【図面の簡単な説明】

【図１】

図１は、本発明の一実施形態が適用されたセキュリティ仕様書作成支援装置１１により、設計対象システム１６に対するコンポジットセキュリティ仕様書原案が作成されるまでの大まかな処理の流れ（原理）を示す図である。

【図２】

図２は、設計対象システムの一例を示す図である。

【図３】

図３（Ａ）は国際セキュリティ評価基準ＩＳＯ１５４０８準拠セキュリティ仕

様書（ＰＰ/ＳＴ）の構成例３１および各種定義情報の記述例３３を示す図であり、図３（Ｂ）はコンポジットセキュリティ仕様書の一例３５を示す図である。

【図４】

図４は、本実施形態のセキュリティ仕様書作成支援装置１１の概略図である。

【図５】

図５は、セキュリティ仕様書事例ＤＢ５４３のデータ管理の仕組みを説明するための図である。

【図６】

図６は、システム構成事例ＤＢ５４４の登録例を示す図である。

【図７】

図７は、運用環境事例ＤＢ５４５の登録例を示す図である。

【図８】

図８は、本実施形態のセキュリティ仕様書作成支援装置１１の動作フローを説明するための図である。

【図９】

図９は、図８のＳ７１１での処理（設計対象システムの定義情報の受付・登録）の詳細なフローを示す図である。

【図１０】

図１０（Ａ）～図１０（Ｄ）は、システム構成定義ＰＧ５４２１が表示装置５６に表示する作業画面のメニューバーの一例を示す図である。

【図１１】

図１１は、システム構成定義ＰＧ５４２１が表示装置５６に表示するＴＯＥ定義画面９２の一例を示す図である。

【図１２】

図１２は、システム構成定義ＰＧ５４２１が表示装置５６に表示するドメイン定義画面９３の一例を示す図である。

【図１３】

図１３は、システム構成定義ＰＧ５４２１が表示装置５６に表示するサブシステム定義画面９４の一例を示す図である。

【図１４】

図１４は、システム構成定義ＰＧ５４２１が表示装置５６に表示するコンポーネント定義画面９５の一例を示す図である。

【図１５】

図１５は、セキュリティ仕様書選定ＰＧ５４２２が表示装置５６に表示する再利用可能事例画面９６の一例を示す図である。

【図１６】

図１６は、セキュリティ仕様書原案作成ＰＧ５４２３が表示装置５６に表示するセキュリティ仕様書作成・編集画面９７の一例を示す図である。

【図１７】

図１７は、セキュリティ仕様書原案作成ＰＧ５４２３が表示装置５６に表示するセキュリティ仕様書作成・編集画面９７の一例を示す図である。

【図１８】

図１８は、セキュリティ仕様書作成支援装置１１の変形例を示す図である。

【符号の説明】

１１･･･セキュリティ設計支援装置、５１･･･ＣＰＵ、５２･･･端末入出力装置、５３･･･バス、５４･･･外部記憶装置、５５･･･メモリ、５６･･･表示装置、５７･･･入力装置、５８･･･ネットワークＩＦ装置、５９･･･可搬記憶媒体入出力装置、５４１･･･通信制御ＰＧ、５４２･･･セキュリティ仕様書作成支援ＰＧ、５４３･･･セキュリティ仕様書事例ＤＢ、５４４･･･システム構成事例ＤＢ、５４５･･･運用環境事例ＤＢ、５５１･･･運用環境事例格納領域、５５２･･･システム構成事例格納領域、５５３･･･セキュリティ仕様書事例格納領域、５５４･･･設計対象システム定義情報格納領域、５５５･･･セキュリティ仕様書原案格納領域、５９１･･･可搬記憶媒体、５４２１･･･システム構成定義ＰＧ、５４２２･･･セキュリティ仕様書選定ＰＧ、５４２３･･･セキュリティ仕様書原案作成ＰＧ

【書類名】図面

【図１】

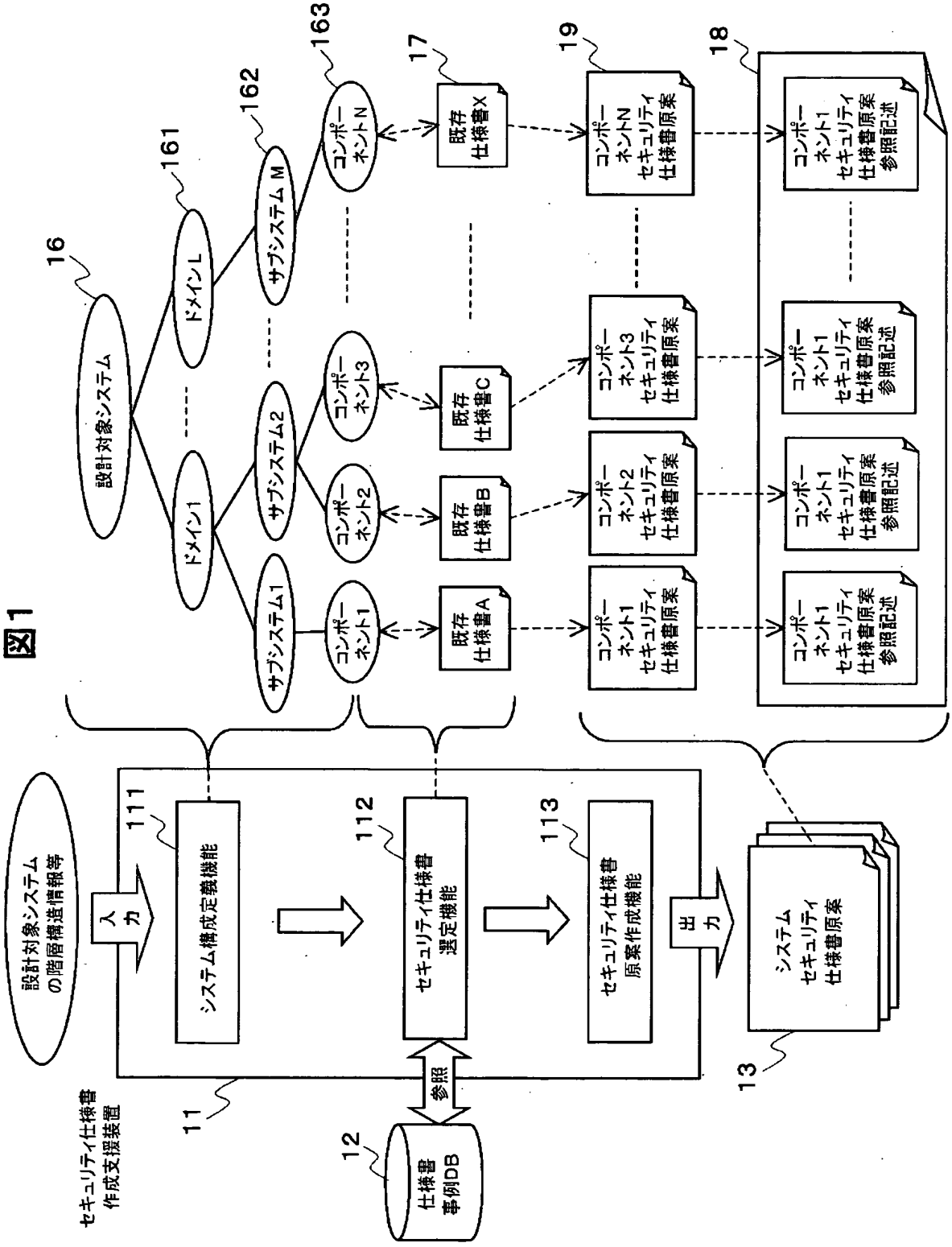


図1
設計対象システム
の階層構造情報等
入力
システム構成定義機能
111
セキュリティ仕様書
選定機能
112
セキュリティ仕様書
原案作成機能
113
出力
システム
セキュリティ
仕様書原案
13
セキュリティ仕様書
作成支援装置
11
参照
仕様書
事例DB
12
設計対象システム
16
ドメイン1
ドメインL
161
サブシステム1
サブシステム2
サブシステムM
162
コンポーネント1
コンポーネント2
コンポーネント3
コンポーネントN
163
既存
仕様書A
既存
仕様書B
既存
仕様書C
既存
仕様書X
17
コンポーネント1
セキュリティ
仕様書原案
コンポーネント2
セキュリティ
仕様書原案
コンポーネント3
セキュリティ
仕様書原案
コンポーネントN
セキュリティ
仕様書原案
19
コンポーネント1
セキュリティ
仕様書原案
参照記述
コンポーネント1
セキュリティ
仕様書原案
参照記述
コンポーネント1
セキュリティ
仕様書原案
参照記述
コンポーネント1
セキュリティ
仕様書原案
参照記述
18

【図２】

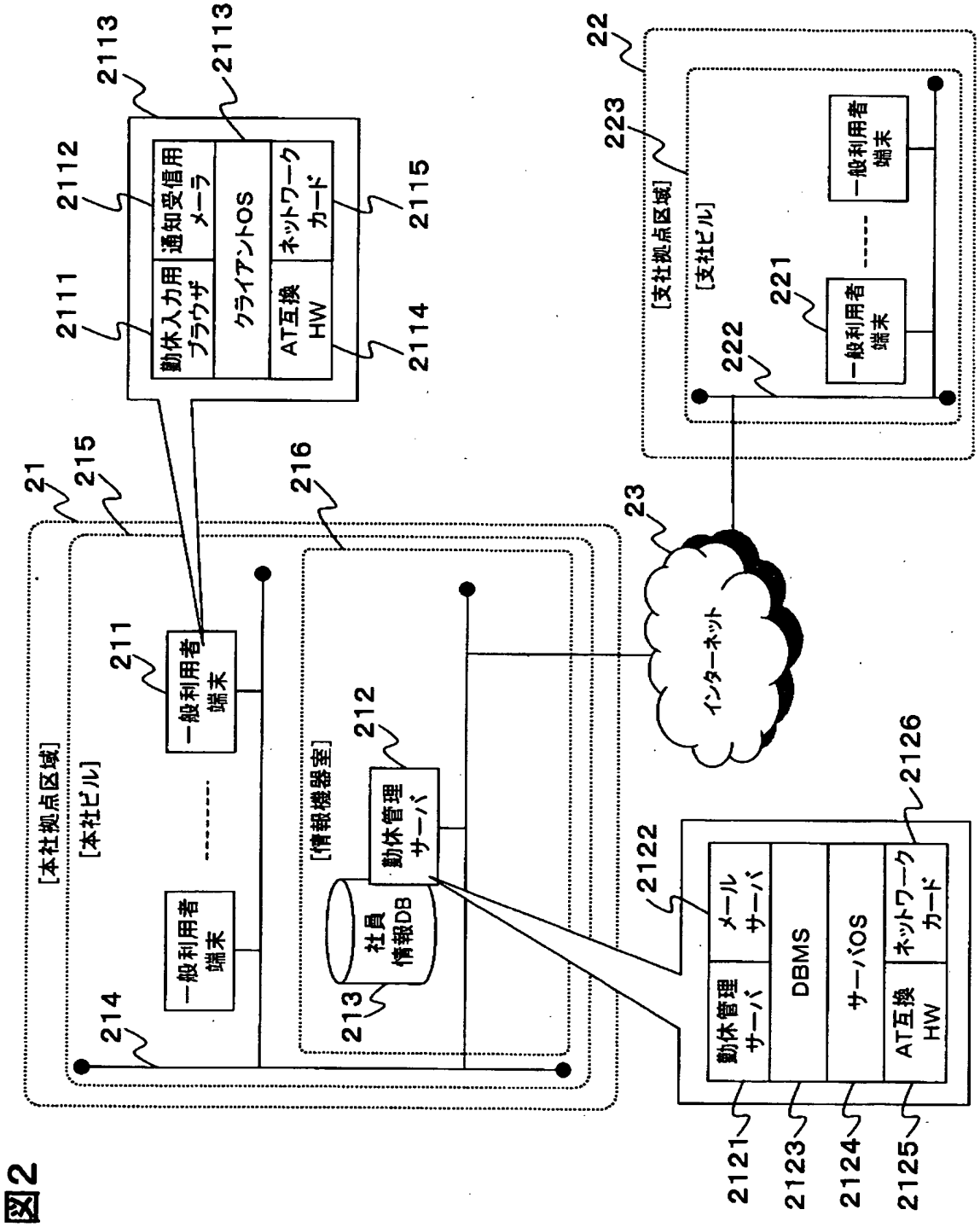

[本社拠点区域]
[本社ビル]
[情報機器室]
[支社拠点区域]
[支社ビル]
一般利用者端末
勤休管理サーバ
社員情報DB
インターネット
勤休入力用ブラウザ
通知受信用メーラ
クライアントOS
AT互換HW
ネットワークカード
メールサーバ
DBMS
サーバOS
21
211
212
213
214
215
216
22
221
222
223
23
2111
2112
2113
2114
2115
2121
2122
2123
2124
2125
2126

図2

【図３】

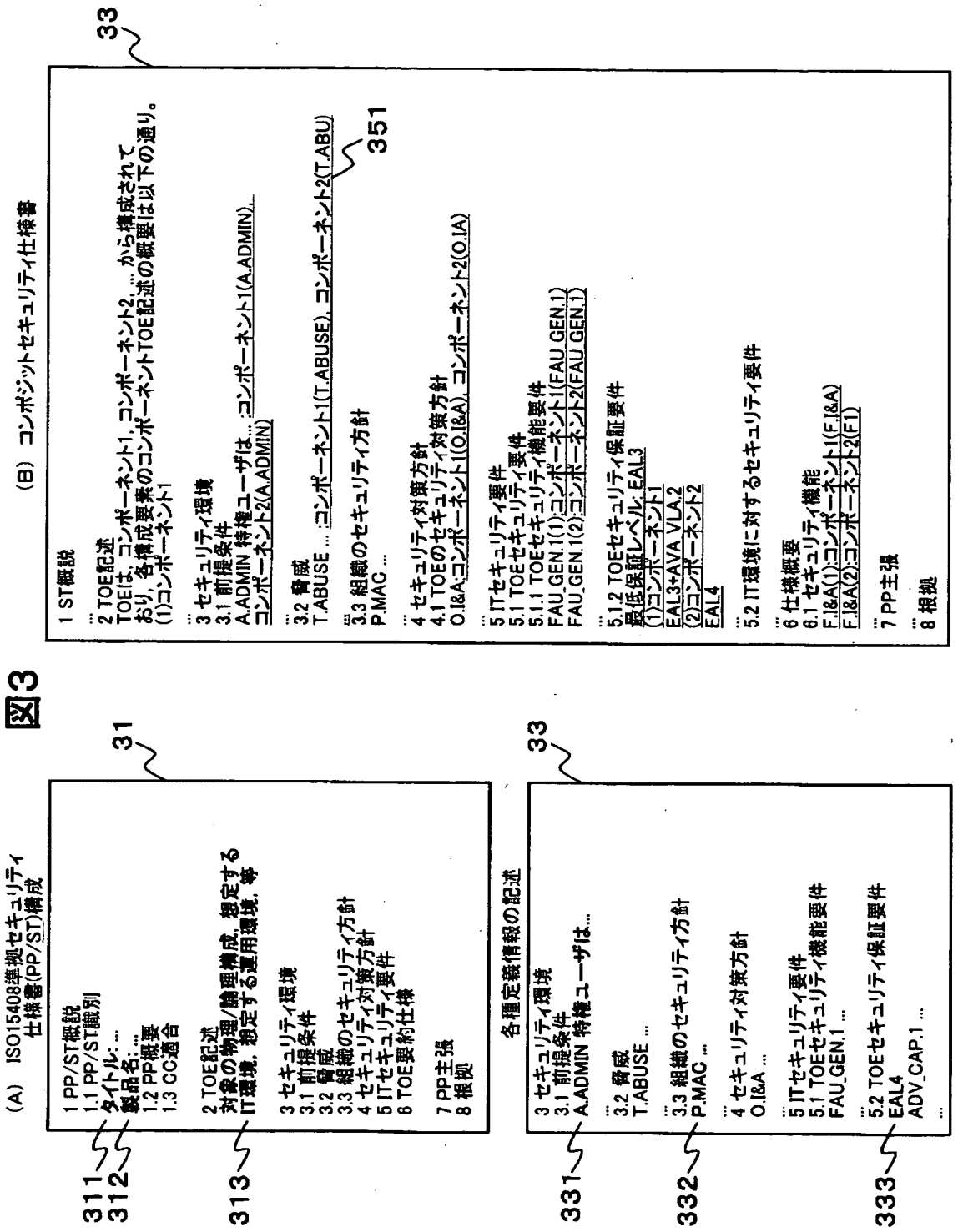


図3
(A) ISO15408準拠セキュリティ仕様書(PP/ST)構成
1 PP/ST概説
1.1 PP/ST識別
タイトル; ...
製品名; ...
1.2 PP概要
1.3 CC適合
2 TOE記述
対象の物理/論理構成, 想定する IT環境, 想定する運用環境, 等
3 セキュリティ環境
3.1 前提条件
3.2 脅威
3.3 組織のセキュリティ方針
4 セキュリティ対策方針
5 ITセキュリティ要件
6 TOE要約仕様
7 PP主張
8 根拠
31
311
312
313
各種定義情報の記述
3 セキュリティ環境
3.1 前提条件
A.ADMIN 特権ユーザは...
...
3.2 脅威
T.ABUSE ...
...
3.3 組織のセキュリティ方針
P.MAC ...
...
4 セキュリティ対策方針
O.I&A ...
...
5 ITセキュリティ要件
5.1 TOEセキュリティ機能要件
FAU_GEN.1 ...
...
5.2 TOEセキュリティ保証要件
EAL4
ADV_CAP.1 ...
...
33
331
332
333
(B) コンポジットセキュリティ仕様書
1 ST概説
...
2 TOE記述
TOEは, コンポーネント1, コンポーネント2, ... から構成されており, 各構成要素のコンポーネントTOE記述の概要は以下の通り。
(1)コンポーネント1
...
3 セキュリティ環境
3.1 前提条件
A.ADMIN 特権ユーザは, ...:コンポーネント1(A.ADMIN),
コンポーネント2(A.ADMIN)
...
3.2 脅威
T.ABUSE ...:コンポーネント1(T.ABUSE), コンポーネント2(T.ABU)
...
3.3 組織のセキュリティ方針
P.MAC ...
...
4 セキュリティ対策方針
4.1 TOEのセキュリティ対策方針
O.I&A:コンポーネント1(O.I&A), コンポーネント2(O.IA)
...
5 ITセキュリティ要件
5.1 TOEセキュリティ要件
5.1.1 TOEセキュリティ機能要件
FAU_GEN.1(1):コンポーネント1(FAU_GEN.1)
FAU_GEN.1(2):コンポーネント2(FAU_GEN.1)
...
5.1.2 TOEセキュリティ保証要件
最低保証レベル: EAL3
(1)コンポーネント1
EAL3+AVA_VLA.2
(2)コンポーネント2
EAL4
...
5.2 IT環境に対するセキュリティ要件
...
6 仕様概要
6.1 セキュリティ機能
F.I&A(1):コンポーネント1(F.I&A)
F.I&A(2):コンポーネント2(F1)
...
7 PP主張
...
8 根拠
351

【図４】

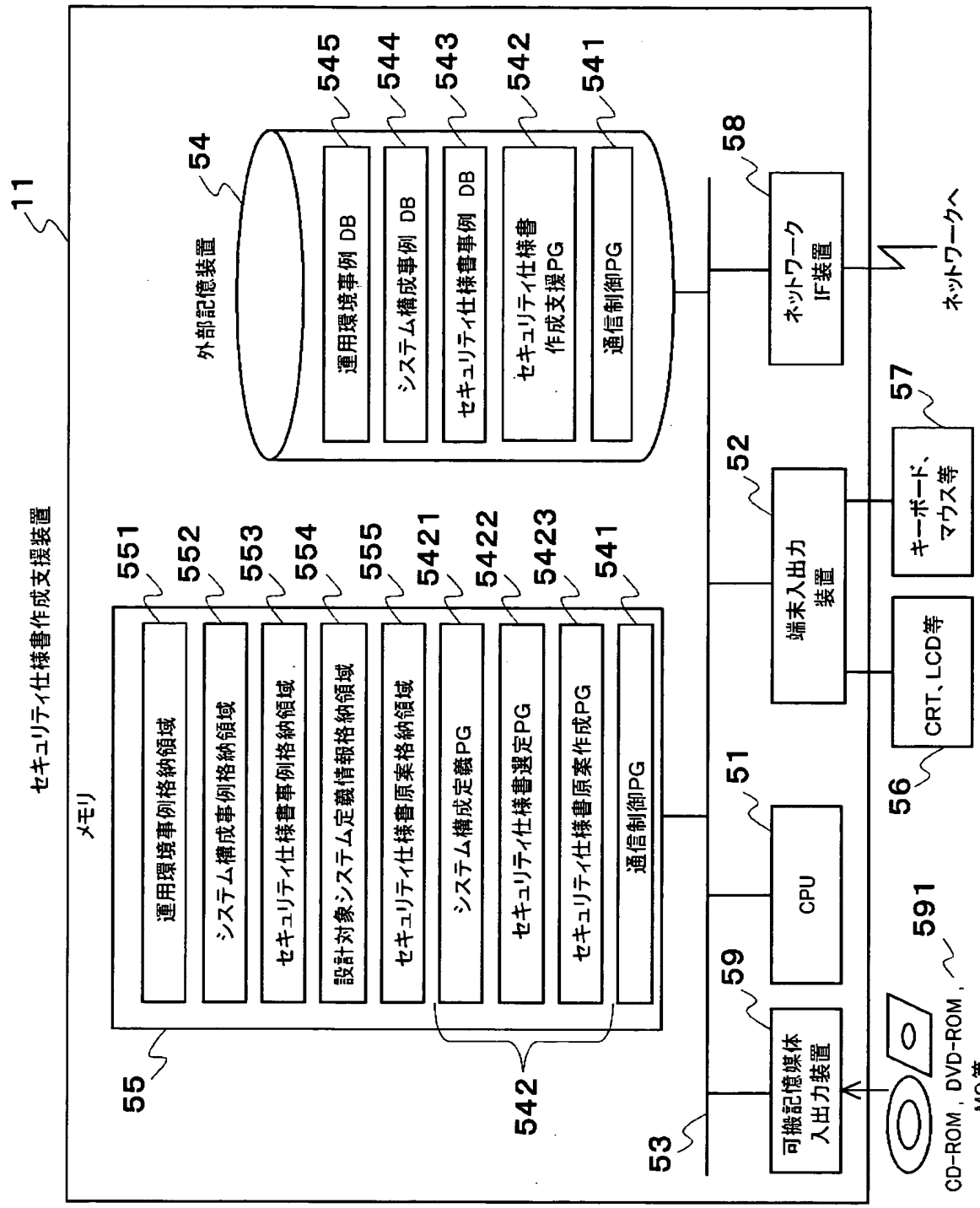
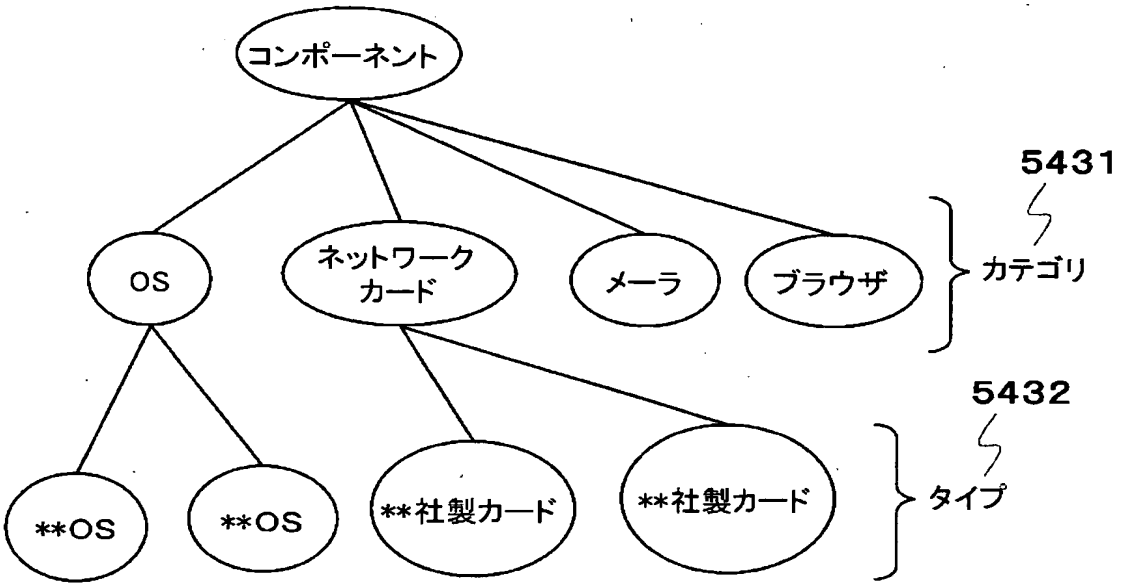

11
セキュリティ仕様書作成支援装置
メモリ
55
551 運用環境事例格納領域
552 システム構成事例格納領域
553 セキュリティ仕様書事例格納領域
554 設計対象システム定義情報格納領域
555 セキュリティ仕様書原案格納領域
5421 システム構成定義PG
5422 セキュリティ仕様書選定PG
5423 セキュリティ仕様書原案作成PG
541 通信制御PG
542
54 外部記憶装置
545 運用環境事例 DB
544 システム構成事例 DB
543 セキュリティ仕様書事例 DB
542 セキュリティ仕様書作成支援PG
541 通信制御PG
53
51 CPU
52 端末入出力装置
56 CRT、LCD等
57 キーボード、マウス等
58 ネットワークIF装置
ネットワークへ
59 可搬記憶媒体入出力装置
591 CD-ROM，DVD-ROM，MO等

図4

【図５】

図５



セキュリティ仕様書事例DB543

【図６】

図6

システム構成事例DB544

<サブシステム >　5443a
<要素名 >IT機器</要素名 >　5446
<コンポーネント >
<要素名 >アプリケーション層 </要素名 >
</コンポーネント >
<コンポーネント >　5444a
<要素名 >ミドルウェア層 </要素名 >　5447
</コンポーネント >
<コンポーネント >　5444b
<要素名 >OS層</要素名 >
</コンポーネント >
<コンポーネント >
<要素名 >ハードウェア層 </要素名 >
</コンポーネント >
</サブシステム >　5443b

5441
システム展開パターン

<サブシステム >
<要素名 >ICカード</要素名 >
<コンポーネント >
<要素名 >アプリケーション層 </要素名 >
</コンポーネント >
<コンポーネント >
<要素名 >OS層</要素名 >
</コンポーネント >
<コンポーネント >
<要素名 >ハードウェア層 </要素名 >
</コンポーネント >
</サブシステム >

<サブシステム >
<要素名 >H社ICカード</要素名 >
<コンポーネント >
<要素名 >アプリケーション </要素名 >
<定義文 ></定義文 >
<仕様書 ></仕様書 >
</コンポーネント >
<コンポーネント >
<要素名 >ICカードOS</要素名 >
<定義文 >本ICカードOSは，…</定義文 >
<仕様書 >"A社 ICカードOS ST v2.0 "</仕様書 >
</コンポーネント >
<コンポーネント >
<要素名 >ICチップ</要素名 >
<定義文 >本ICチップは，…</定義文 >
<仕様書 >"H社 ICチップ ST v1.1 "</仕様書 >
</コンポーネント >
</サブシステム >

【図７】

図7

運用環境事例DB545

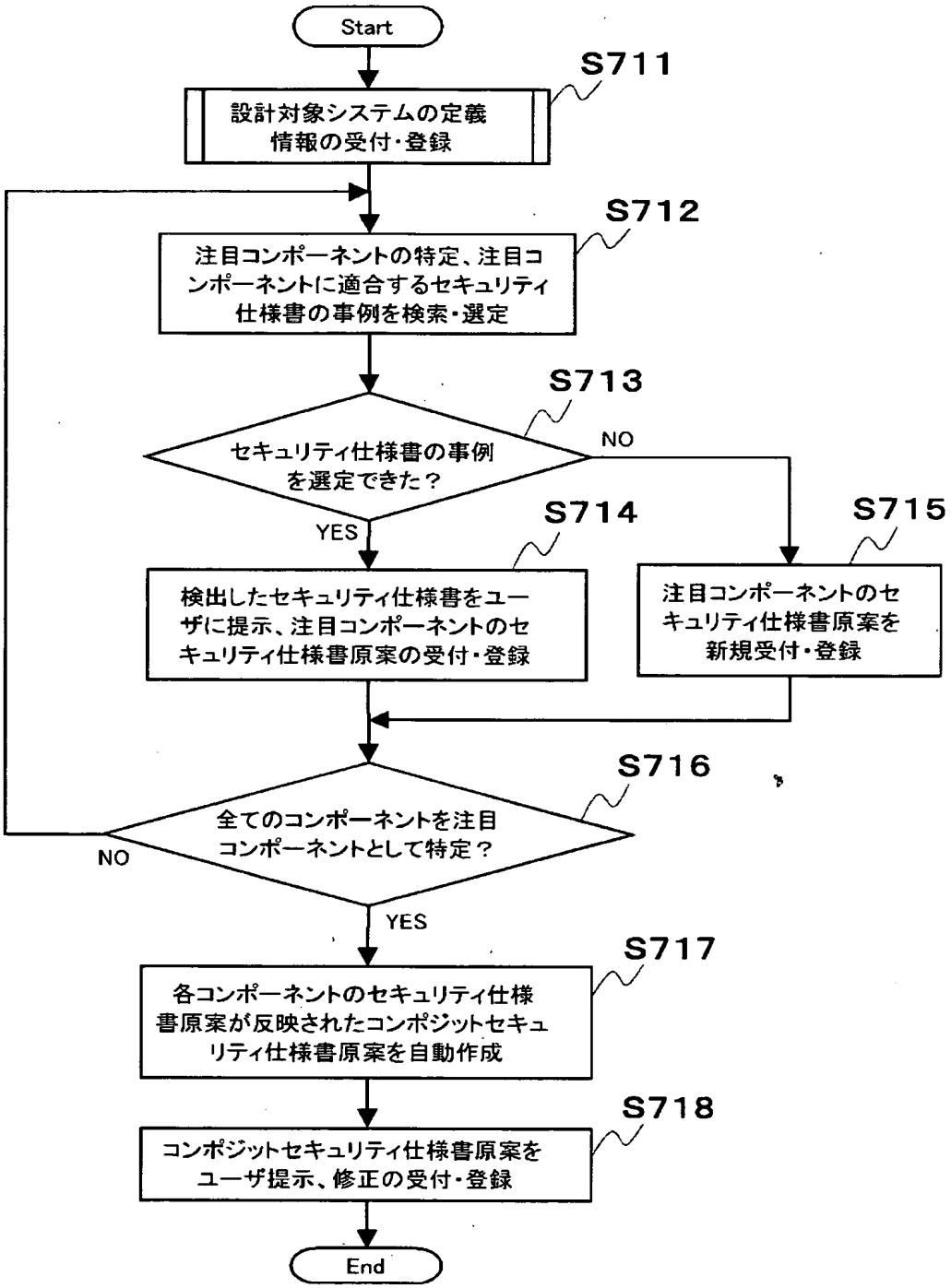
<サブシステム >
<要素名 >IT機器</要素名 >　　5452
<運用>パスワードの機密性を確保するように運用する。　</運用>
<コンポーネント >
<要素名 >アプリケーション層 </要素名 >
<運用>パスワードは，入力時に画面上に表示しない。　</運用>
<運用>パスワードを紙などに可読な状態で記録しておかない。　</運用>
…
</コンポーネント >
<コンポーネント >
<要素名 >OS層</要素名 >
<運用>パスワードは，入力時に画面上に表示しない。　</運用>
<運用>パスワードを紙などに可読な状態で記録しておかない。　</運用>
<運用>パスワードを定期的に変更する。 </運用>
…
</コンポーネント >
</サブシステム >

<サブシステム >
…
</サブシステム >

5451
運用環境パターン

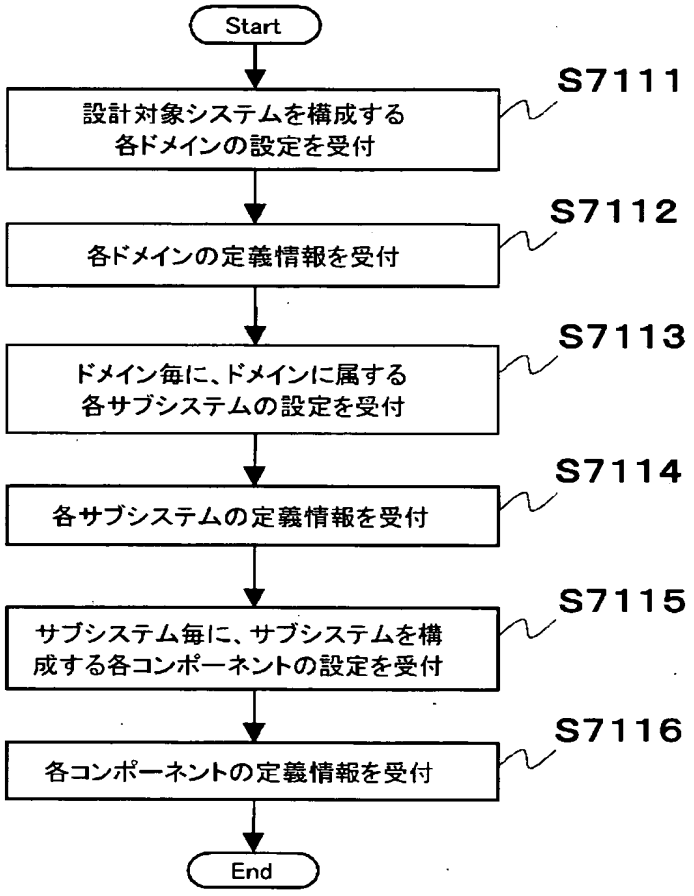
【図８】

図8


Start
S711
設計対象システムの定義情報の受付・登録
S712
注目コンポーネントの特定、注目コンポーネントに適合するセキュリティ仕様書の事例を検索・選定
S713
セキュリティ仕様書の事例を選定できた？
NO
YES
S714
検出したセキュリティ仕様書をユーザに提示、注目コンポーネントのセキュリティ仕様書原案の受付・登録
S715
注目コンポーネントのセキュリティ仕様書原案を新規受付・登録
S716
全てのコンポーネントを注目コンポーネントとして特定？
NO
YES
S717
各コンポーネントのセキュリティ仕様書原案が反映されたコンポジットセキュリティ仕様書原案を自動作成
S718
コンポジットセキュリティ仕様書原案をユーザ提示、修正の受付・登録
End

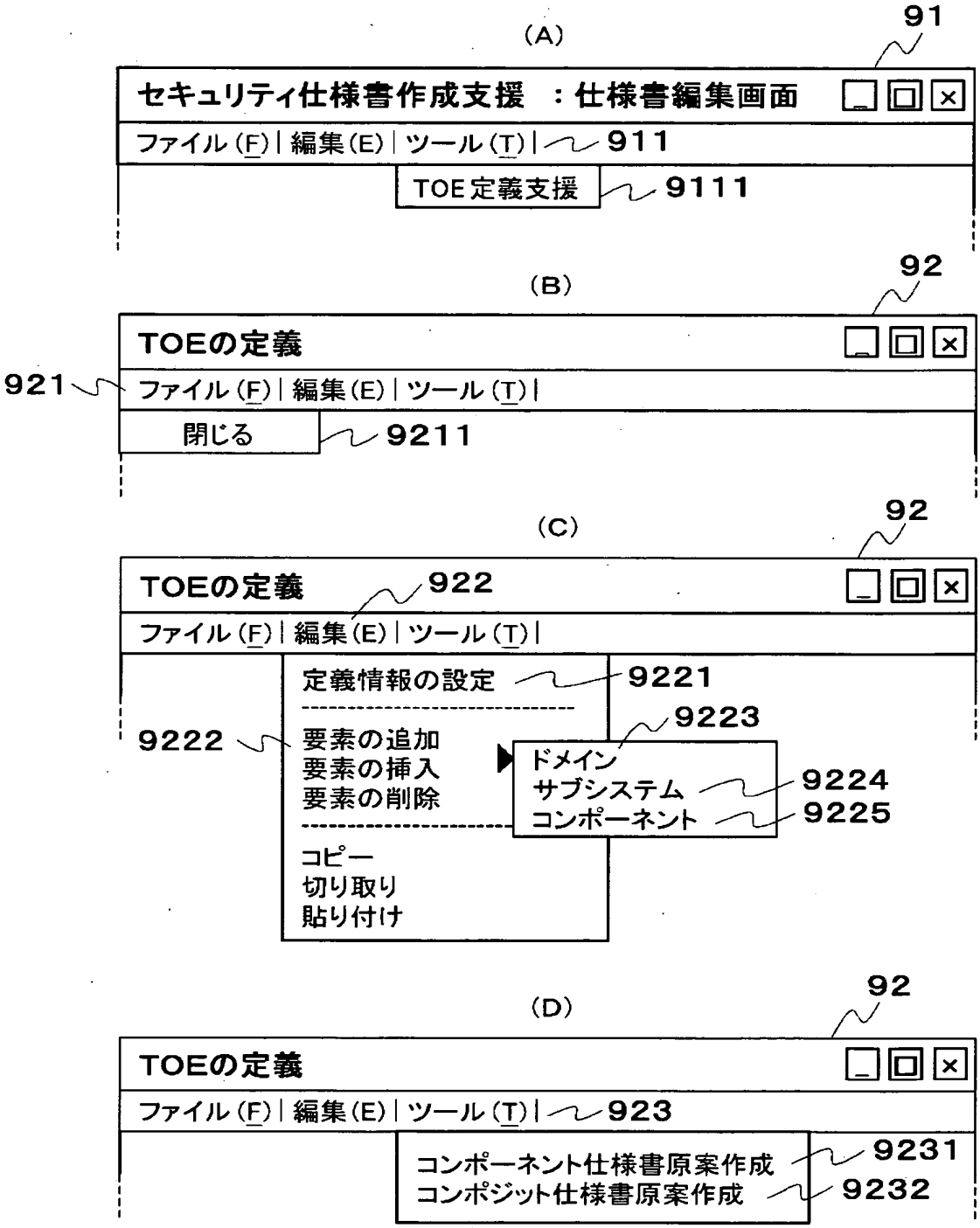
【図９】

図9


Start
設計対象システムを構成する
各ドメインの設定を受付
S7111
各ドメインの定義情報を受付
S7112
ドメイン毎に、ドメインに属する
各サブシステムの設定を受付
S7113
各サブシステムの定義情報を受付
S7114
サブシステム毎に、サブシステムを構
成する各コンポーネントの設定を受付
S7115
各コンポーネントの定義情報を受付
S7116
End

【図１０】

図10


(A)
91
セキュリティ仕様書作成支援　：仕様書編集画面
ファイル(F)|編集(E)|ツール(T)|
911
TOE定義支援
9111
(B)
92
TOEの定義
921
ファイル(F)|編集(E)|ツール(T)|
閉じる
9211
(C)
92
TOEの定義
922
ファイル(F)|編集(E)|ツール(T)|
定義情報の設定
9221
9223
9222
要素の追加
要素の挿入
要素の削除
ドメイン
サブシステム
コンポーネント
9224
9225
コピー
切り取り
貼り付け
(D)
92
TOEの定義
ファイル(F)|編集(E)|ツール(T)|
923
コンポーネント仕様書原案作成
コンポジット仕様書原案作成
9231
9232

【図１１】

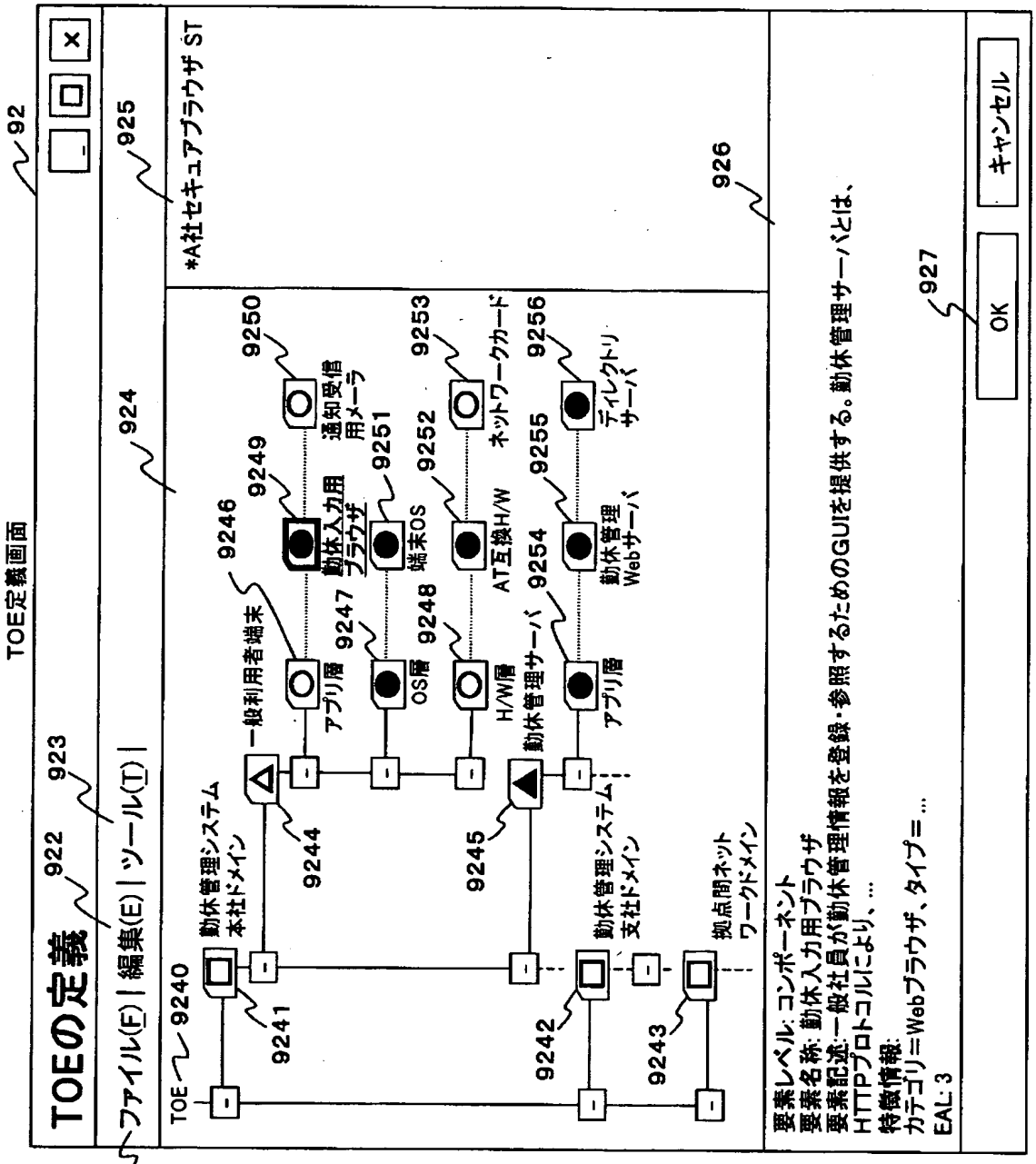

TOE定義画面
92
TOEの定義
922
923
ファイル(F) | 編集(E) | ツール(T) |
921
924
925
*A社セキュアブラウザ ST
926
927
TOE
9240
9241
9242
9243
9244
9245
9246
9247
9248
9249
9250
9251
9252
9253
9254
9255
9256
動休管理システム 本社ドメイン
動休管理システム 支社ドメイン
拠点間ネットワークドメイン
一般利用者端末
動休管理サーバ
アプリ層
OS層
H/W層
動休入力用ブラウザ
通知受信用メーラ
端末OS
AT互換H/W
ネットワークカード
ディレクトリサーバ
動休管理Webサーバ
要素レベル: コンポーネント
要素名称: 動休入力用ブラウザ
要素記述: 一般社員が動休管理情報を登録・参照するためのGUIを提供する。動休管理サーバとは、HTTPプロトコルにより、...
特徴情報:
カテゴリ=Webブラウザ、タイプ=...
EAL: 3
OK
キャンセル

図１１

【図１２】

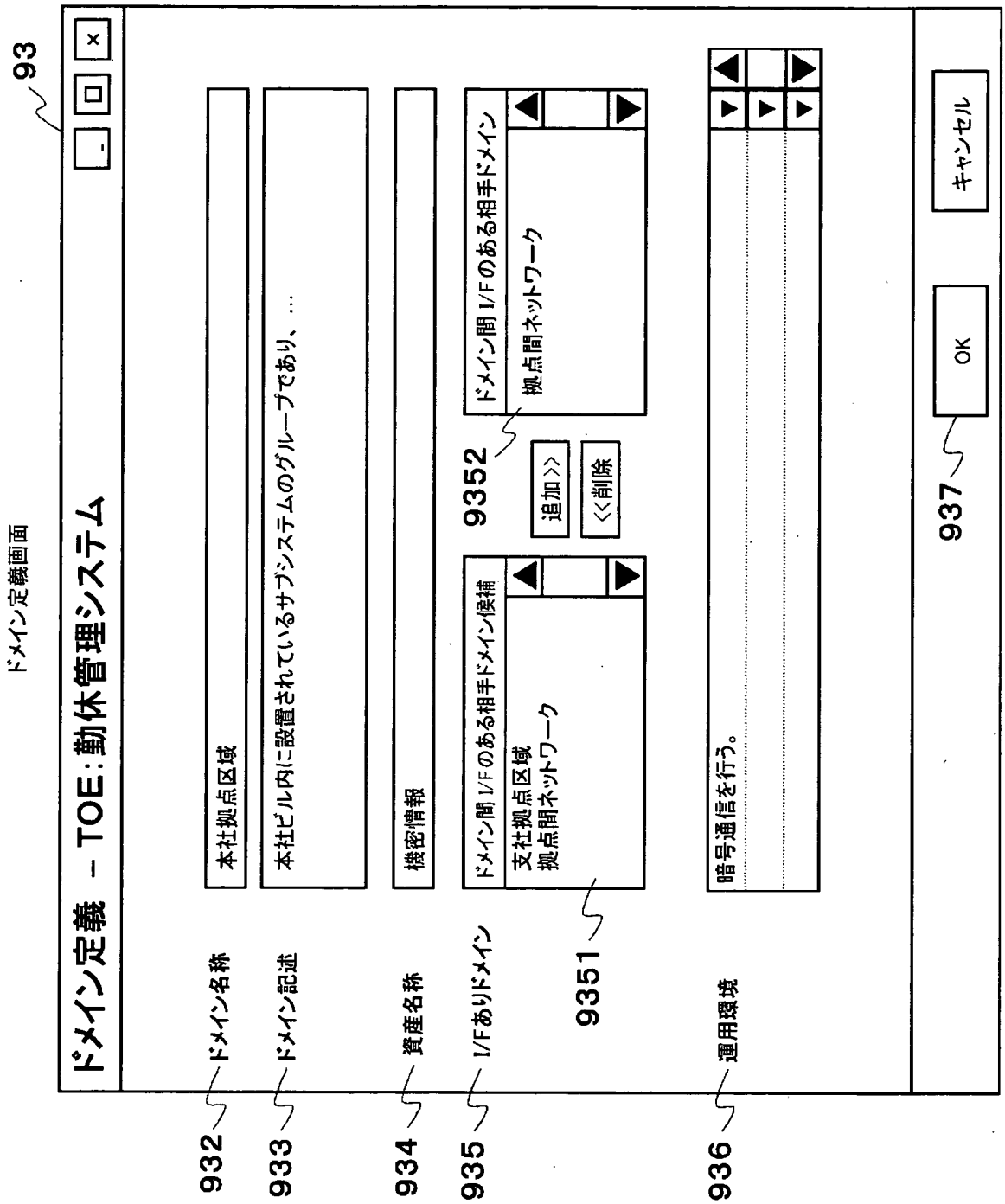

ドメイン定義画面
93
ドメイン定義 － TOE：勤休管理システム
ドメイン名称
本社拠点区域
932
ドメイン記述
本社ビル内に設置されているサブシステムのグループであり、…
933
資産名称
機密情報
934
I/Fありドメイン
ドメイン間 I/Fのある相手ドメイン候補
支社拠点区域
拠点間ネットワーク
9351
935
追加>>
<<削除
ドメイン間 I/Fのある相手ドメイン
拠点間ネットワーク
9352
運用環境
暗号通信を行う。
936
OK
キャンセル
937

図12

【図１３】

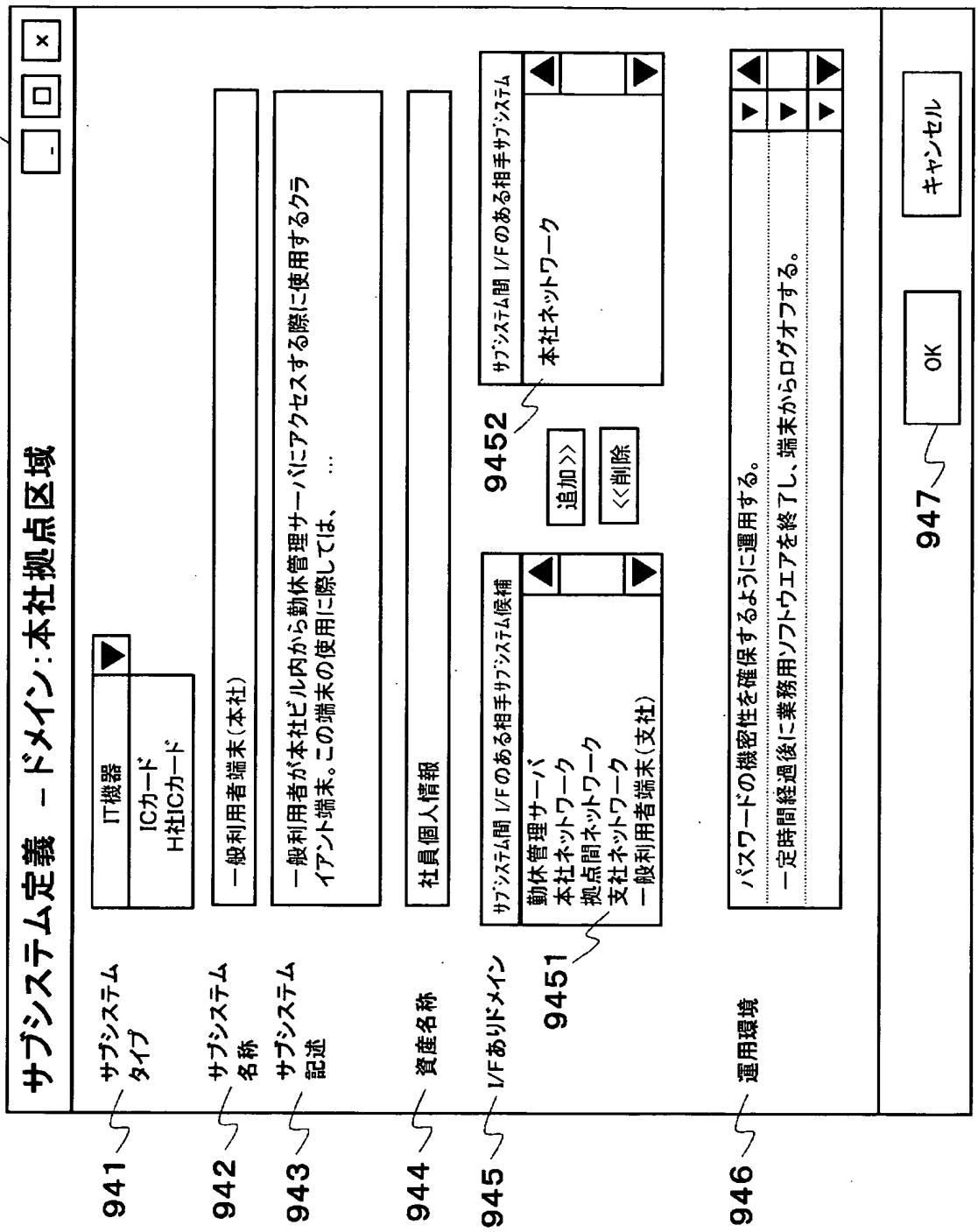

サブシステム定義画面
94
サブシステム定義　－ドメイン：本社拠点区域
サブシステム タイプ
IT機器
ICカード
H社ICカード
941
サブシステム 名称
一般利用者端末（本社）
942
サブシステム 記述
一般利用者が本社ビル内から勤休管理サーバにアクセスする際に使用するクライアント端末。この端末の使用に際しては、…
943
資産名称
社員個人情報
944
I/Fありドメイン
サブシステム間 I/Fのある相手サブシステム候補
勤休管理サーバ
本社ネットワーク
拠点間ネットワーク
支社ネットワーク
一般利用者端末（支社）
9451
追加>>
<<削除
サブシステム間 I/Fのある相手サブシステム
本社ネットワーク
9452
945
運用環境
パスワードの機密性を確保するように運用する。
一定時間経過後に業務用ソフトウエアを終了し、端末からログオフする。
946
947
OK
キャンセル

図13

【図１４】

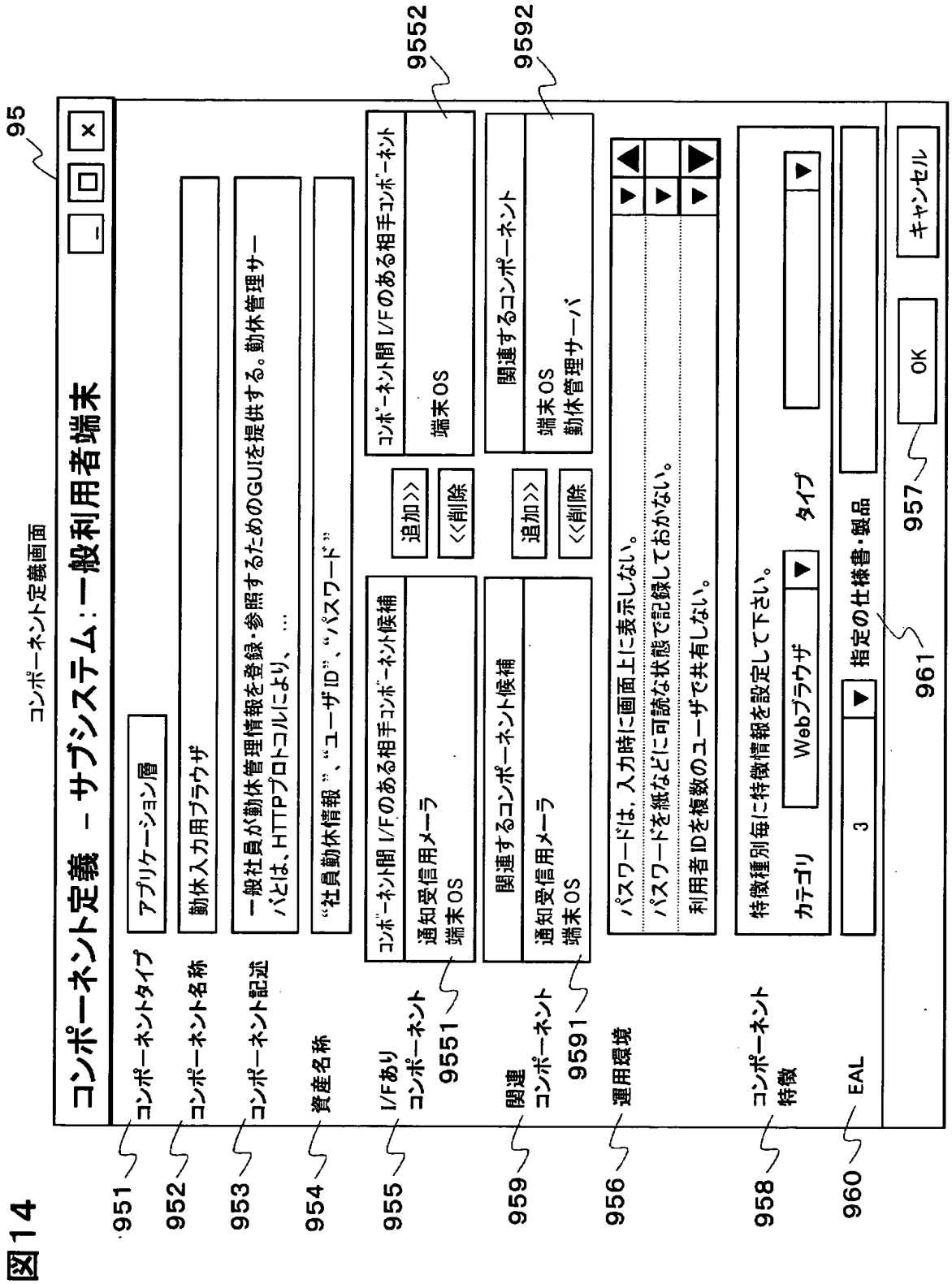
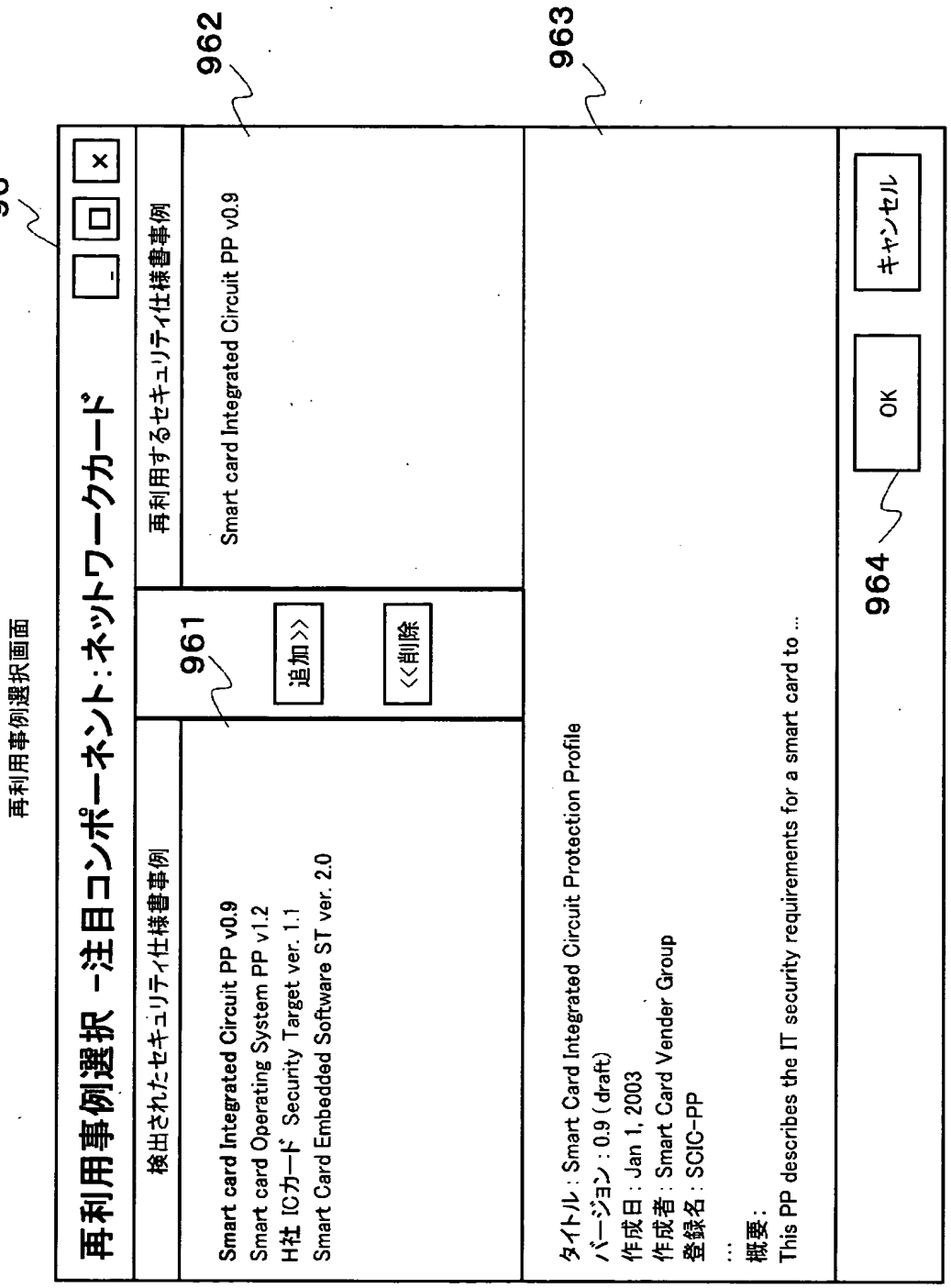


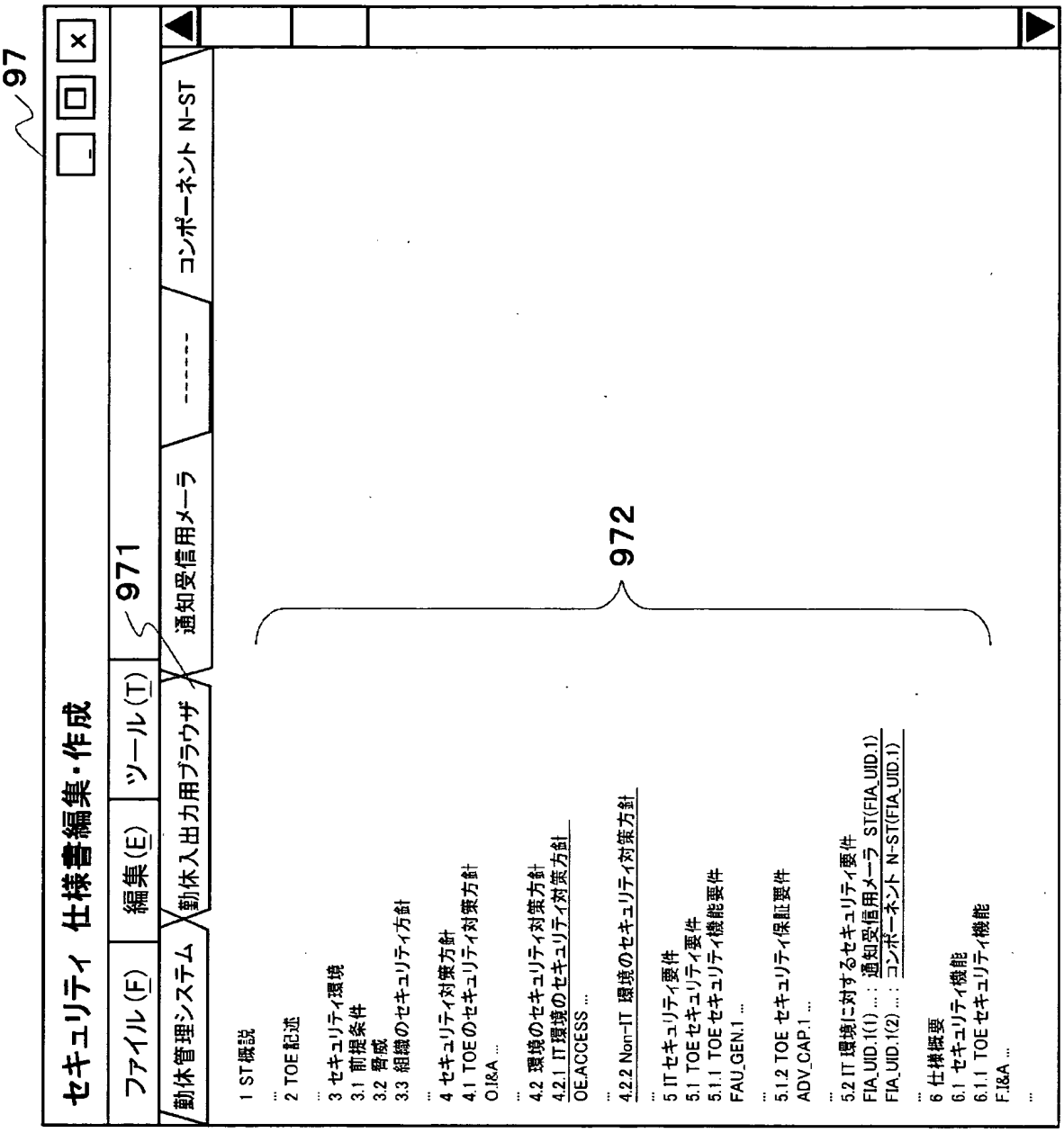
図14
コンポーネント定義画面
95
コンポーネント定義 － サブシステム:一般利用者端末
951
コンポーネントタイプ
アプリケーション層
952
コンポーネント名称
勤休入力用ブラウザ
953
コンポーネント記述
一般社員が勤休管理情報を登録・参照するためのGUIを提供する。勤休管理サーバとは、HTTPプロトコルにより、…
954
資産名称
“社員勤休情報”、“ユーザID”、“パスワード”
955
I/Fあり
コンポーネント
9551
コンポーネント間 I/Fのある相手コンポーネント候補
通知受信用メーラ
端末OS
追加>>
<<削除
9552
コンポーネント間 I/Fのある相手コンポーネント
端末OS
959
関連
コンポーネント
9591
関連するコンポーネント候補
通知受信用メーラ
端末OS
追加>>
<<削除
9592
関連するコンポーネント
端末OS
勤休管理サーバ
956
運用環境
パスワードは，入力時に画面上に表示しない。
パスワードを紙などに可読な状態で記録しておかない。
利用者IDを複数のユーザで共有しない。
958
コンポーネント
特徴
特徴種別毎に特徴情報を設定して下さい。
カテゴリ
Webブラウザ
タイプ
960
EAL
3
指定の仕様書・製品
961
957
OK
キャンセル

【図１５】

図15


96
再利用事例選択画面
再利用事例選択 -注目コンポーネント:ネットワークカード
検出されたセキュリティ仕様書事例
961
Smart card Integrated Circuit PP v0.9
Smart card Operating System PP v1.2
H社 ICカード Security Target ver. 1.1
Smart Card Embedded Software ST ver. 2.0
追加>>
<<削除
再利用するセキュリティ仕様書事例
962
Smart card Integrated Circuit PP v0.9
963
タイトル : Smart Card Integrated Circuit Protection Profile
バージョン : 0.9 (draft)
作成日 : Jan 1, 2003
作成者 : Smart Card Vender Group
登録名 : SCIC-PP
...
概要 :
This PP describes the IT security requirements for a smart card to ...
964
OK
キャンセル

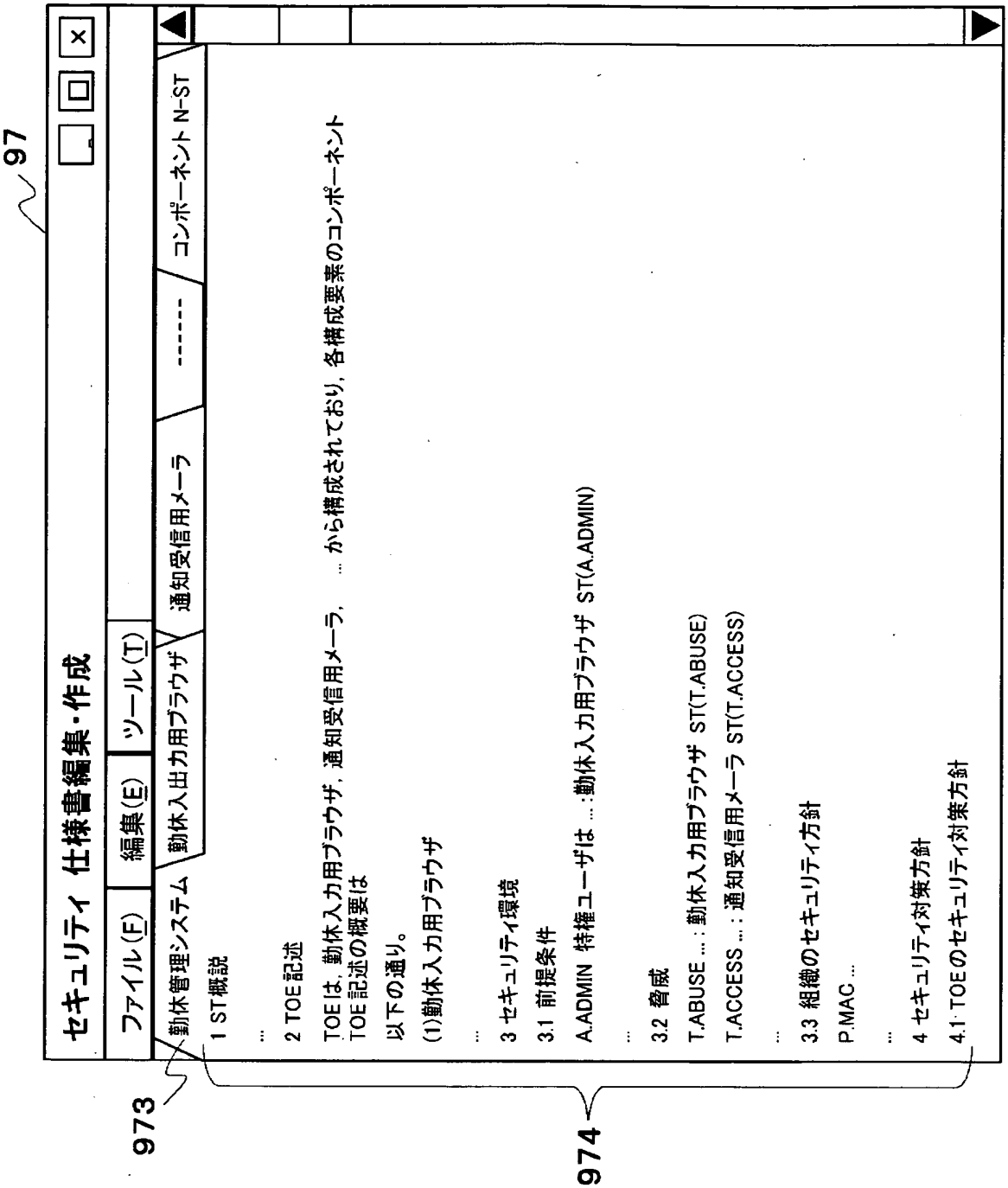
【図１６】


97
セキュリティ 仕様書編集・作成
ファイル(F)
編集(E)
ツール(T)
971
勤休管理システム
勤休入出力用ブラウザ
通知受信用メーラ

コンポーネント N-ST
1 ST概説
...
2 TOE記述
...
3 セキュリティ環境
3.1 前提条件
3.2 脅威
3.3 組織のセキュリティ方針
...
4 セキュリティ対策方針
4.1 TOEのセキュリティ対策方針
O.I&A ...
...
4.2 環境のセキュリティ対策方針
4.2.1 IT環境のセキュリティ対策方針
OE.ACCESS ...
...
4.2.2 Non-IT 環境のセキュリティ対策方針
...
5 ITセキュリティ要件
5.1 TOEセキュリティ要件
5.1.1 TOEセキュリティ機能要件
FAU_GEN.1 ...
...
5.1.2 TOE セキュリティ保証要件
ADV_CAP.1 ...
...
5.2 IT 環境に対するセキュリティ要件
FIA_UID.1(1) ... : 通知受信用メーラ ST(FIA_UID.1)
FIA_UID.1(2) ... : コンポーネント N-ST(FIA_UID.1)
...
6 仕様概要
6.1 セキュリティ機能
6.1.1 TOEセキュリティ機能
F.I&A ...
...
972

図16

【図１７】


97
セキュリティ 仕様書編集・作成
ファイル(F)
編集(E)
ツール(T)
勤休管理システム
勤休入出力用ブラウザ
通知受信用メーラ

コンポーネント N-ST
973
974
1 ST概説
...
2 TOE記述
TOEは，勤休入力用ブラウザ，通知受信用メーラ，　... から構成されており，各構成要素のコンポーネント
TOE記述の概要は
以下の通り。
(1)勤休入力用ブラウザ
...
3 セキュリティ環境
3.1 前提条件
A.ADMIN 特権ユーザは ...:勤休入力用ブラウザ ST(A.ADMIN)
...
3.2 脅威
T.ABUSE ...:勤休入力用ブラウザ ST(T.ABUSE)
T.ACCESS ...:通知受信用メーラ ST(T.ACCESS)
...
3.3 組織のセキュリティ方針
P.MAC ...
...
4 セキュリティ対策方針
4.1 TOEのセキュリティ対策方針

図17

【図１８】

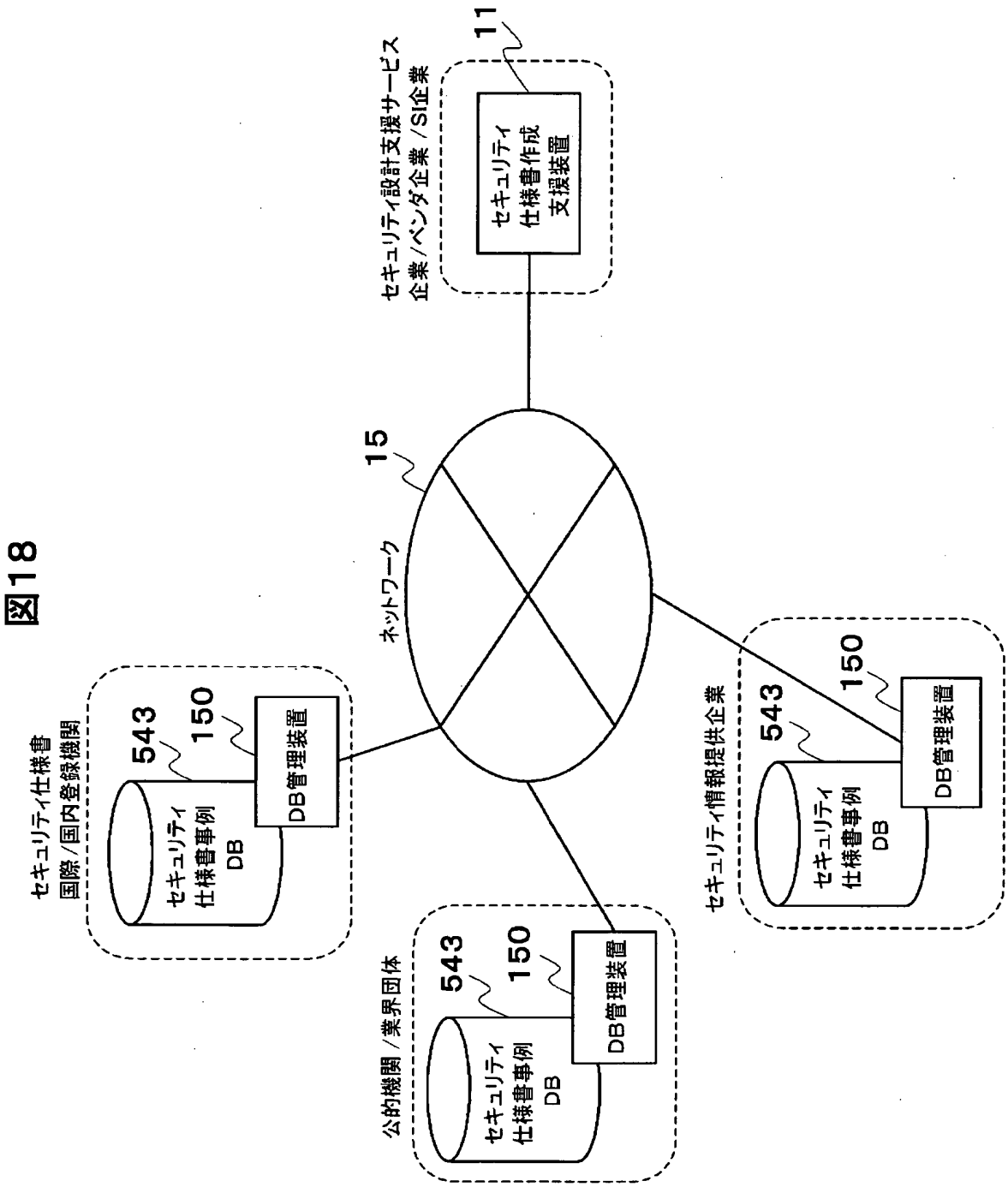


図18
セキュリティ設計支援サービス
企業/ベンダ企業/SI企業
11
セキュリティ
仕様書作成
支援装置
15
ネットワーク
セキュリティ仕様書
国際/国内登録機関
543
150
セキュリティ
仕様書事例
DB
DB管理装置
公的機関/業界団体
543
150
セキュリティ
仕様書事例
DB
DB管理装置
セキュリティ情報提供企業
543
150
セキュリティ
仕様書事例
DB
DB管理装置

【書類名】要約書

【要約】

【課題】複数のＩＴ製品で構成される情報ネットワークシステムに対するセキュリティ仕様書の作成を支援する。

【解決手段】セキュリティ仕様書作成支援装置１１において、システム構成定義ＰＧ５４２１は、設計対象システムを構成する各コンポーネントの定義情報をユーザより受付ける。セキュリティ仕様書選定ＰＧ５４２２は、コンポーネント各々について、セキュリティ仕様書事例ＤＢ５４３に再利用可能なセキュリティ仕様書が存在するか否かを調べ、存在するならばこれを特定する。そして、セキュリティ仕様書原案作成ＰＧ５４２３は、予め用意してあるセキュリティ仕様書の雛形に、特定したセキュリティ仕様書各々の内容を反映して、設計対象システムに対するコンポジットセキュリティ仕様書の原案を自動生成する。

【選択図】図４

特願２００３－１３４７０６

出願人履歴情報

識別番号　［０００００５１０８］

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所